Hybrid Extraterritoriality in Data Regulation

King Fung Tsang*

Sagi Peari**

I. Introduction

Extraterritoriality in cross-border regulation is both a necessity and a source of tension. Data has become strategically important to states around the world for technological competition, privacy protection, crime investigation, economic development, and national security.[1] In the absence of a worldwide regulatory framework backed by effective international enforcement, states have increasingly found it necessary to extend their national laws extraterritorially to data and to the intermediaries controlling such data abroad. This inevitably generates tension among states, particularly conflicts between their respective regulatory regimes. Among the major powers, whose companies control much of this strategically important data, regulatory competition has intensified significantly over the last decades. The extraterritorial regulation of data also has significant implications for private actors, as the effectiveness of modern data regulation increasingly depends on private individuals enforcing their rights and businesses implementing regulatory obligations across borders.

The extraterritoriality of data regulation has attracted extensive attention from practitioners and commentators. Major jurisdictions, including the United States, China, and the European Union (the "EU"), have increasingly developed new private forms of extraterritorial regulation to avoid or mitigate traditional public international law scrutiny. Under these emerging hybrid mechanisms, part of the traditional direct public regulation is effectively transferred to private enforcement. One advantage of this approach is that it may reduce traditional cross-state objections, the breach of which may signal unacceptable extraterritoriality and invite coordinated resistance from other states.

As a result of private regulation, the effectiveness of modern data regulation increasingly depends upon who may sue, where proceedings may be brought, what law governs the dispute, and whether resulting obligations may ultimately be recognized and enforced across borders. These questions, all traditionally associated with a discipline called 'private international law' in a broad sense, therefore occupy an increasing role in modern data regulation.

Public regulation, however, is not displaced by private enforcement. Rather, modern data regulation increasingly operates through hybrid combinations of public regulation and private international law mechanisms to constitute a new form of extraterritoriality. Although the United States, the EU, and China all make use of such mechanisms, they do so divergently in light of their respective regulatory priorities and strategic interests concerning data. The resulting system in each jurisdiction is a distinctive combination of public regulation and private international law techniques, designed both to advance its own regulatory objectives and to defend against competing forms of extraterritorial regulation adopted by other jurisdictions.

---

* Associate Professor, The Chinese University of Hong Kong; SJD (Georgetown); LLM & JD (Columbia).

** Associate Professor of Private and Commercial Law, University of Western Australia. Professor Tsang contributed 90% to the article, while Associate Professor Peari contributed 10%. The authors would like to thank Hei Yin Leung for his excellent research assistance. This research was generously supported by the Hong Kong Chief Executive's Policy Unit under the Public Policy Research Funding Scheme 2025–26 (Project No. 2025.A4.121.25C).

[1] In this article, the terms "data," "information," and "knowledge" are used interchangeably unless otherwise indicated. Data is defined broadly, covering personal data, technical data, and government data.

The article seeks to achieve the following two interrelated goals. First, it aims to identify and analyze the emerging form of hybrid extraterritoriality, which combines traditional cross-border public regulation with private international law mechanisms. Second, it aims to flesh out a new understanding of private international law through its focus on data extraterritoriality, examining how it could form part of private international law operational dynamics.

To achieve these objectives, the article examines and compares the approaches to extraterritorial data regulation adopted by the United States, the EU, and China. These jurisdictions are chosen not only because of their significant economic power and regulatory influence, but also because of the unique way in which those states increasingly take account of the others' regulatory regimes in designing their own. In particular, each jurisdiction has developed defensive mechanisms, including blocking statutes and localization measures, to resist or mitigate the extraterritorial reach of competing regimes. Taken together, these jurisdictions form an interconnected regulatory ecosystem that is simultaneously competitive and interdependent.

Section II examines the nature of data regulation, explaining how data may be effectively regulated under national law, including through the regulation of intermediaries, and how such regulation may extend extraterritorially. It further explores the nature of extraterritoriality and argues that, while traditionally associated with public international law, modern cross-border data regulation increasingly operates through a hybrid combination of public regulation and private enforcement, thereby making private international law increasingly relevant. Section III suggests learning from the shortcomings of the famous Siberian Pipeline dispute in the early 1980s to illustrate the traditional public-law model of extraterritorial regulation and its limitations. The dispute, which concerned the U.S. prohibition on the transfer of technical data and components by U.S. subsidiaries in Europe for the construction of the Siberian Pipeline, and the strong opposition this provoked within the European Economic Community, may be viewed as one of the earliest major cross-border disputes involving data regulation.

Section IV epitomizes the core of the argument by examining four major features of modern extraterritorial data regulation. It begins with regulations which restrict cross-border data transfers, using examples including Executive Order 14117 of the United States and the Standard Contractual Clauses ("SCCs") under both the General Data Protection Regulation ("GDPR") [2] and Chinese data laws. It then examines regulations which regulate the extraterritorial use of personal data. These include the GDPR and Chinese data laws, as well as relevant state statutes and common law doctrines in the United States. The article goes on to consider regulations that are designed to retrieve or compel disclosure of data located abroad. The principal example is the CLOUD Act, followed by the EU's forthcoming E-Evidence regime. Finally, the article examines defense mechanisms, principally blocking statutes and data localization measures. Taken together, these four forms of regulation structure, as argued, the international legal ecosystem governing cross-border data regulation.

Section V concludes by drawing together the respective approaches of the three jurisdictions toward the emerging hybrid form of extraterritoriality. The thrust of the argument is that the United States has pursued the most expansive regulatory objectives. Although generally making comparatively less use of private enforcement mechanisms, it has increasingly relied on private international law techniques in different forms. The EU occupies an intermediate position, making extensive use of private enforcement and private international law

[2] 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

mechanisms while maintaining comparatively balanced regulatory objectives. China's regulatory approach shares certain similarities with the EU, but departs more sharply with respect to sensitive data, localization, conflict avoidance, and defensive regulation, reflecting a stronger emphasis on security and sovereign control.

II. Data Regulation, Extraterritoriality, and Public-Private International Law Divide

Data comes in many shapes and forms, but perhaps its most striking feature is the ease with which it can be transmitted from one country to another.[3] It may therefore create the impression that national law, which is territorial in nature, cannot efficiently regulate something like data, which can be stored, transmitted, and divided in any country in the world.[4]

According to Professors Jack Goldsmith and Tim Wu, a state can regulate conduct within its territory effectively if it can control any one of the "source," "intermediary," and "target."[5] Applying this insight to Internet regulation, they argue that intermediaries, particularly "the ISPs (Internet Service Providers), search engines, browsers, the physical network, and financial intermediaries" are not eliminated by the rise of the Internet,[6] and that governments can control local intermediaries within their territory in order to achieve effective regulation of the Internet.[7]

The same analytical framework applies to the closely related problem of data regulation. A state can regulate the data itself, which is the source for present purposes, the intermediaries, which substantially overlap with those in the Internet analysis, and the end users of data (the target) within its jurisdiction. Like Internet regulation, modern data regulation increasingly relies upon regulating data processors as the principal intermediaries through which regulatory objectives are achieved. This is especially true for the stronger economic powers in the world, such as the United States, the EU, and China, which exercise control over many intermediaries operating worldwide.[8] Such control enables states to apply their data laws even where the data or the relevant data subject is located abroad. However, while foreign private parties may ultimately be required to comply with such regulation, the extraterritorial application of a state's law has traditionally been regarded as an interference with the sovereign authority of the state in whose territory the person or property is located.

This gives rise to the perplexed question of extraterritoriality. It is frequently unclear what commentators consider to be subject to extraterritoriality. Is it a person, property, or conduct located in a foreign country? Some commentators even suggest abolishing the use of the term entirely.[9]

---

[3] Paul Schiff Berman, *Legal Jurisdiction and the Deterritorialization of Data*, 71 Vand. L. Rev. En Banc 11, 23 (2018).

[4] *Id*. at 23 (arguing that "[t]erritorial location of data or servers is irrelevant").

[5] Jack Goldsmith & Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* 69 (2006).

[6] *Id*. at 70.

[7] *Id*.

[8] Goldsmith & Wu, *supra* note 5, at 81–82. As will be further discussed in Section IV, controlling intermediaries is not the only approach. States also seek to control both source data, despite its transmissible nature, and the end users of data through national law, since all of these have physical locations and may therefore be subject to territorial regulation. Taken together, this makes data a matter that can be regulated effectively by national law.

[9] Andreas F. Lowenfeld, *International Litigation and the Quest for Reasonableness: General Course on Private International Law*, 245 Recueil des Cours 9, 44 (1994).

One way to define extraterritoriality is to begin with the three axioms of Huber, who is widely regarded as the founding father of modern private international law.[10] According to Huber, a country's laws have effect only within its own borders and therefore, as a general rule, have no extraterritorial effect.[11] However, under Huber's third axiom, it is possible for another country, Country B, voluntarily to apply Country A's law. This is the famous doctrine of comity.[12] Accordingly, if one state willingly gives extraterritorial effect to another state's law, that is still a form of extraterritoriality, but not the type prohibited under Huber's first axiom. Thus, extraterritoriality based on this territorial theory of jurisdiction is summarized by Story and restated by Mann as follows: "No State can, by its laws, directly affect or bind property out of its own territory or bind persons not resident therein."[13] Over time, changes in the modern world have given rise to demands for exceptions.[14] A number of doctrines have accordingly emerged which are said to justify, i.e. render lawful, the extraterritorial application of a state's law. These include the passive personality, universality, effects, and nationality principles.[15] Of these, nationality principle was already accepted by Huber.[16] Joseph Story's writings in the United States followed a similar trajectory.[17] The first two principles generally apply only in the criminal field and are regarded as weaker justifications.[18] The more controversial doctrine is the effects principle, which continues to evolve and has gained increasing acceptance, particularly in antitrust.[19]

Public and private international law, and the relationship between them, are critical to understanding the nature of extraterritoriality. The former governs disputes between sovereign states, while the latter governs private disputes involving foreign elements.[20] Private international law generally addresses three principal questions: (1) jurisdiction—which court may exercise adjudicatory jurisdiction over a dispute; (2) choice of law—which system of domestic law the court should apply; and (3) the recognition and enforcement of foreign judgments—whether the court should give effect to a foreign judgment through its recognition and enforcement.[21]

---

[10] D.J. Llewelyn Davies, *The Influence of Huber's De Conflictu Legum on English Private International Law*, 18 *Brit. Y.B. Int'l L.* 49 (1937).

[11] The first two axioms provide that each state's laws are effective only within its own territory. See Ulrik Huber, *De Conflictu Legum Diversarum in Diversis Imperiis* (1689), discussed in Davies, *supra* note 10, at 49.

[12] As Mann pointed out, the territoriality theory—the first two axioms—is probably the most important contribution of Huber's principles, *see* F.A. Mann, The Doctrine of Jurisdiction in International Law, 111 Recueil des Cours 1, 27 (1964).

[13] In Story's original wording, the definition is "No State can, by its laws, directly affect or bind property out of its own territory or bind persons not resident therein, except that every nation has a right to bind its own subjects by its own laws in every other place." However, as Mann rightly pointed out, "[t]he expression is not entirely correct in that the extension of jurisdiction to non-resident nationals introduces an element which lacks territorial character." In other words, the proviso in the second principle should be deleted, because it mixes up what constitutes extraterritoriality with the justification for it. See Mann, *The Doctrine of Jurisdiction*, supra note 12, at 28.

[14] Mann, *The Doctrine of Jurisdiction*, *supra* note 12, at 36–40.

[15] James Crawford, *Brownlie's Principles of Public International Law* 443-455 (9th ed. Oxford Univ. Press 2019).

[16] *See supra* notes 10–11, 17.

[17] Joseph Story, *Commentaries on the Conflict of Laws, Foreign and Domestic* (1st ed. 1834) (extending the nationality principle to non-resident citizens).

[18] Mann, *The Doctrine of Jurisdiction*, *supra* note 12, at 40.

[19] T.C. Hartley, *The Modern Approach to Private International Law: International Litigation and Transactions from a Common-Law Perspective*, 319 *Recueil des Cours* 9 (2006).

[20] Peter Hay, Patrick J. Borchers, Symeon C. Symeonides & Christopher A. Whytock, *Conflict of Laws* 2 (6th ed. 2018).

[21] P.M. North & J.J. Fawcett, *Cheshire and North's Private International Law* 1 (11th ed. 1987); Lord Collins of Mapesbury & Jonathan Harris eds., *Dicey, Morris & Collins on the Conflict of Laws* ¶ 1-004 (16th ed. 2022) ; Hay, *id*. at 2.

Whether extraterritoriality belongs to public or private international law has not been clear. Hornbook writers are inconsistent in their treatment. Some seemingly treated extraterritoriality as purely a matter of public international law, while some treated it as a matter for both.[22]

Mann took the latter view but articulated the relationship more clearly as follows:

(i) Public and private international law are distinct but substantially convergent in the context of extraterritoriality.[23]

(ii) More specifically, public international law sets out the outer limits of acceptable extraterritoriality, that is, territorial jurisdiction together with its recognised extensions. Private international law, as national law, may operate within those limits established by public international law.[24]

(iii) Private international law primarily implements rules in the field of private law, whereas public law entails a different set of considerations. Public law areas therefore generally fall outside the scope of private international law and are regulated principally by public international law.[25]

Accordingly, both public and private international law have important roles to play in the regulation of data extraterritorially. Traditionally, extraterritorial regulation has relied primarily on public enforcement, and discussions of extraterritoriality have therefore focused largely on public international law. Modern data regulation operates principally through intermediaries. As the following sections demonstrate, however, modern extraterritorial data regulation increasingly makes use of private enforcement mechanisms against those intermediaries. This development, in turn, gives private international law an increasingly significant role in the implementation of extraterritorial data regulation.

Before turning to the modern hybrid approach, it is useful to examine an earlier model of extraterritorial data regulation: the United States' restriction of technical-data exports in the Siberian Pipeline dispute of the early 1980s. The European Economic Community ("EEC") objected that the U.S. Export Administration Regulations infringed the principle of territoriality, exceeded any permissible nationality-based jurisdiction over corporations, and could not be justified by either the protective principle or the effects doctrine.[26] In the end, the United States rescinded the measures.[27] The dispute is significant because the U.S. measures did not merely regulate physical goods. They also sought to control the transfer and use of pipeline-related technical data abroad. This older model relied primarily on public enforcement against foreign-based intermediaries and on the controversial idea that U.S.-origin technical data could remain subject to U.S. control even after being transferred outside the United States. It was therefore heavily scrutinized under public international law.

The European Economic Community ("EEC") objected that the June 22, 1982 amendments to the U.S. Export Administration Regulations infringed the principle of territoriality, exceeded

---

[22] US textbook writers tend to include extraterritoriality in private international law texts, *see, e.g.*, Hay, *supra* note 20, at 227–266; R. Lea Brilmayer, Jack L. Goldsmith, Erin O'Hara O'Connor & Carlos M. Vázquez, *Conflict of Laws: Cases and Materials* 575–643 (8th ed. 2019) , whereas English conflicts writers tend not to include extraterritoriality, *see, e.g.*, Dicey, *supra* note 22; Cheshire, *supra* note 22.

[23] Mann, *The Doctrine of Jurisdiction*, *supra* note 12, at 23.

[24] *Id*. at 19–20.

[25] *Id*. at 17–18.

[26] European Community: Comments on the Amendments of 22 June 1982 to the United States Export Administration Act, *in* A.V. Lowe, *Extraterritorial Jurisdiction* 201–205 (1983); Aide-Mémoire, *id.* at 216–219.

[27] Andreas F. Lowenfeld, International Litigation and the Quest for Reasonableness: Essays in Private International Law 979–981 (Clarendon Press 1996).

any permissible nationality-based jurisdiction over corporations, and could not be justified by either the protective principle or the effects doctrine.[28] The measures also provoked strong diplomatic opposition and legal countermeasures, including blocking statutes, in several European states. In the end, the United States rescinded the measures.[29] In that sense, the episode was a failed example of direct public law extraterritoriality. At the same time, it provides useful lessons for the modern hybrid approach, discussed in Section IV, which relies more heavily on private international law mechanisms, including particularly contractual submission.

III. A Case Study of the Old Form of Data Extraterritoriality

A. The Siberian Pipeline dispute

The story began with the Siberian Pipeline project, under which several Western European countries and the Soviet Union would cooperate in constructing a pipeline to transport natural gas from Siberia to Western Europe. The project was substantial, reportedly involving approximately $15 billion, an astronomical amount in the early 1980s.[30] Against the background of U.S. opposition to the Soviet Union's role in Poland, and concern that Western Europe would become dependent on Soviet energy supplies, the United States announced an embargo on the export of pipeline-related technology on December 29, 1981.[31] Further measures were imposed on June 22, 1982 (the "June 22 Measures").

In particular, the June 22 Measures extended the embargo in two important respects. First, they extended U.S. export controls to foreign subsidiaries and affiliates of U.S. companies, even where those entities were organized or doing business outside the United States. The measures covered the "export of non-U.S. origin goods and technical data by U.S. owned or controlled companies wherever organized or doing business."[32] Second, they extended U.S. control to certain foreign products derived from U.S.-origin technical data. This included products of U.S. technical data (i) where "the right to the use of the data abroad is subject to a licensing agreement with persons subject to the jurisdiction of the U.S.," (ii) where the use of the data required "the payment of royalties or other compensation" to such persons, or (iii) where "the recipient of the technical data has agreed to abide by U.S. export control regulation."[33]

The June 22 Measures therefore reached beyond U.S. persons and entities. They prohibited not only U.S. companies from exporting technical data relating to pipeline technology to the Soviet Union, but also European subsidiaries of U.S. companies and European companies that had licensed technical data of U.S. origin. The measures were met with strong opposition from the EEC, individual European governments, and private parties.

---

[28] European Community: Comments on the Amendments of 22 June 1982 to the United States Export Administration Act, *in* A.V. Lowe, *Extraterritorial Jurisdiction* 201–205 (1983); Aide-Mémoire, *id.* at 216–219.

[29] Lowenfeld, *supra* note 27.

[30] Patrizio Merciai, *The Euro-Siberian Gas Pipeline Dispute—A Compelling Case for the Adoption of Jurisdictional Codes of Conduct*, 8 Md. J. Int'l L. 1, 2 (1984).

[31] *Id.* at 11.

[32] 15 C.F.R. pts. 376, 379, 385 (1982).

[33] *Id.*

The EEC issued a formal comment criticizing the June 22 Measures as an unjustified exercise of extraterritorial jurisdiction in violation of public international law.[34] It stated that "[t]he American measures clearly infringe the principle of territoriality" because they purported to regulate the activities of companies in the European Community that were outside the territorial competence of the United States.[35] With respect to European subsidiaries of U.S. companies, the EEC argued that the measures could not be justified by the nationality principle. In its view, corporate nationality for this purpose covered only companies that had their place of incorporation or registered office in the United States, and did not extend merely because a European company was owned or controlled by a U.S. parent.[36]

The EEC was even more critical of the attempt to regulate European licensees whose only connection with the United States was their use of U.S.-origin technical data. In response to the premise that technical data could carry U.S. jurisdictional control abroad, the EEC stated that "technology [does] not have any nationality and there are no known rules under international law for using … technology situated abroad as a basis of establishing jurisdiction over the persons controlling [it]."[37] This objection went to the heart of the old model of data extraterritoriality: the United States treated technical data as if its U.S. origin could justify continuing U.S. regulatory control abroad, while the EEC rejected the idea that data or technology could itself provide a basis of extraterritoriality.

The EEC also rejected any reliance on the protective principle or the effects doctrine. As to the protective principle, it argued that the US government had not sought to justify the measures on the basis of national security.[38] In any event, the connection between the embargo of pipeline-related technical data and U.S. security was, from the EEC's perspective, too remote. As to the effects doctrine, the EEC argued that exports from the EEC to the Soviet Union would not produce any "direct, foreseeable and substantial effects" within the United States.[39]

The EEC's public international law objections were accompanied by domestic countermeasures at the national level. The United Kingdom, France, and West Germany reportedly ordered companies within their territories to perform existing pipeline contracts notwithstanding the U.S. embargo. The most noteworthy national measure was the United Kingdom's blocking statute, the Protection of Trading Interests Act.[40] France also adopted its own blocking measure, aimed in particular at restricting the transmission of information to foreign authorities or for use in foreign proceedings.

The UK Act had originally been designed as a response to U.S. antitrust extraterritoriality and became one of the leading early statutory responses to perceived overreach by U.S. extraterritorial regulation. Under section 1(1), the Secretary of State may designate foreign trade-control measures where they apply, or would apply, to things done outside the territorial jurisdiction of the foreign state by persons carrying on business in the United Kingdom, and

---

[34] For a discussion of the formal status of the EEC comments, see A.V. Lowe, *Public International Law and the Conflict of Laws: The European Response to the United States Export Administration Regulations*, 33 *Int'l & Comp. L.Q.* 515, 529–530 (1984).

[35] Lowe, *supra* note 27, at 202.

[36] *See* EEC Comments, Lowe, *supra* note 27, at 202 (citing *Barcelona Traction, Light and Power Co., Ltd. (Belg. v. Spain)*, 1970 I.C.J. 3 (Feb. 5).

[37] EEC Comments, Lowe, *supra* note 27, at 203.

[38] Lowe, *supra* note 27, at 205.

[39] *Id*. at 205.

[40] Protection of Trading Interests Act 1980, c. 11 (U.K.).

where those measures damage or threaten to damage the trading interests of the United Kingdom.[41]

Once designated, the Act sought to counter extraterritorial regulation in three principal ways. It may require persons carrying on business in the United Kingdom not to comply with the foreign measure[42] and prohibit compliance with requests for documents or information by overseas courts or authorities ("non-compliance");[43] prevent UK courts from enforcing foreign judgments resulting from the foreign measure ("denial of judgment enforcement");[44] and, where applicable, allow recovery of multiple damages awarded abroad ("claw-back provision").[45]

In the Siberian Pipeline dispute, the UK government used the Act to order UK subsidiaries of U.S. companies not to comply with the pipeline-related technical-data embargo.[46] Soon afterward, the U.S. position softened and the ban was effectively lifted.[47]

Resistance to the embargo also appeared in private litigation. In the United States, a French subsidiary of a U.S. company sought injunctive relief against the application of the embargo to it, but a federal district court rejected the challenge.[48] The more revealing litigation, for present purposes, occurred in Europe. In a Dutch case, a supplier that was an indirect subsidiary of a Texas company was required to perform its contractual obligations to a French company notwithstanding the U.S. embargo.[49] The supplier apparently invoked the US embargo as a basis for non-performance, but the Dutch court held that the U.S. embargo could not constitute a valid *force majeure* defence because, in the court's view, the June 22 Measures were contrary to public international law.[50]

Several lessons can be drawn from the Siberian Pipeline dispute: (1) Public International Law as a Signal of Excessive Extraterritoriality, (2) Private International Law Supplies the Operational Mechanism, and (3) The Untested Private-Law Component of U.S. Data Extraterritoriality.

B. The Lessons of the Siberian Pipeline Dispute

1. Public International Law as a Signal of Excessive Extraterritoriality

Public international law is often criticized for lacking a centralized enforcement mechanism. Violations may go unpunished, and this has led some commentators to question whether treaties and customary international law impose genuine legal obligations in the same way as domestic law.[51] Professors Goldsmith and Posner go further and argue that many classic

---

[41] *Id*. § 1(1).

[42] *Id*. § 1(3).

[43] *Id.* § 2(1).

[44] *Id.* § 5.

[45] *Id.* § 6. *see also* A.V. Lowe, *Blocking Extraterritorial Jurisdiction: The British Protection of Trading Interests Act, 1980*, 75 Am. J. Int'l L. 257, 257 (1981) [hereinafter Lowe, *Blocking Extraterritorial Jurisdiction*].

[46] Lowe, *supra* note 27, at 213.

[47] Lowenfeld, *supra* note 28, at 981.

[48] *Dresser Indus., Inc. v. Baldridge*, 549 F. Supp. 108 (D.D.C. 1982).

[49] *Compagnie Européenne des Pétroles S.A. v. Sensor Nederland B.V*. (District Court at The Hague Sept. 17, 1982), 22 I.L.M. 66 (1983).

[50] *Id*. ¶¶ 5–8.

[51] A Theory of Customary International Law, 66 U. CHI. L. REV. 1113, 1116 (1999).

examples of customary international law may be explained not by states' sense of legal obligation, but by coincidence of interest: "a pattern of behaviour … results from each state acting in its self-interest without any regard to the action of the other state."[52]

Even accepting much of this realist critique, the Siberian Pipeline dispute shows that public international law can still exert an indirect disciplining effect on extraterritoriality. Its importance lies less in direct enforcement than in signalling. A measure that falls outside the recognized bases of legislative jurisdiction, such as territoriality, nationality, the protective principle, or the effects doctrine, becomes easier for other states to characterize as excessive. That characterization, in turn, may help coordinate diplomatic protest, domestic blocking statutes, and private litigation, with the latter two arguably falling within the ambit of private international law.

This is precisely what happened in the Siberian Pipeline dispute. As a matter of domestic law, both the United States and,[53] ironically, the United Kingdom accept that legislation may have extraterritorial effect where the legislature has clearly expressed that intention.[54] But that domestic law proposition does not answer the separate public international law question whether the exercise of extraterritorial jurisdiction is justified internationally. The EEC's objection to the June 22 Measures supplied a common legal vocabulary for condemning the U.S. embargo as excessive. Although the EEC itself did not, or perhaps could not, directly invalidate the U.S. measures, its position helped frame and legitimize the responses of individual European states.

The first lesson, therefore, is that direct public law extraterritoriality is likely to invite public international law scrutiny, especially where the asserted jurisdictional basis is weak. Public international law may not itself provide the final enforcement mechanism, but it can operate as a signal that mobilizes other forms of resistance. The more ambitious the desired extraterritorial regulatory effect, the more likely the measure is to provoke private international law opposition.

2. Private International Law Supplies the Operational Mechanism

If public international law supplies the signal of excessive extraterritoriality, domestic private international law mechanisms supply the teeth. The Protection of Trading Interests Act, discussed above, was not itself public international law. It was not a treaty or rule of customary international law, but a domestic statute of the United Kingdom. Its importance lay in the fact that it translated objections to foreign extraterritoriality into domestic legal consequences: commands not to comply with foreign measures, restrictions on the provision of documents and information to foreign authorities, non-enforcement of certain foreign judgments, and recovery of multiple damages. Unlike public enforcement measures, these mechanisms operate through the regulation of private rights and obligations rather than through direct regulatory sanctions.

Public international law may provide the outer limits of permissible legislative jurisdiction, but those limits usually become operational through national law. The reverse is also true. Where a state's extraterritorial regulation exceeds the limits recognized by public international law, the primary resistance will usually come not from an international court, but from the domestic legal systems of other states. That resistance often takes a private international law form

---

[52] Jack L. Goldsmith & Eric A. Posner, *The Limits of International Law* 12 (2005).

[53] Restatement (Fourth) of Foreign Relations Law § 406 (Am. L. Inst. 2018).

[54] *Assange v. Swedish Prosecution Authority* [2012] UKSC 22, [2012] 2 A.C. 471 (appeal taken from Eng.).

because it concerns the domestic effect of foreign law, foreign proceedings, foreign judgments, and foreign regulatory demands.

Blocking statutes, such as the UK Protection of Trading Interests Act, are a prime example. Under the broader conception of private international law adopted in this article, they may properly be categorized as a part of private international law. Just as importantly, they matter in practice. They may not eliminate the foreign law, but they can discourage extraterritoriality or reduce the effectiveness of the foreign measure. The lesson of the Siberian Pipeline dispute is therefore not that private international law matters while public international law does not. Rather, the successful defensive tactic combined both. Public international law identified the excessive character of the U.S. measures; domestic private international law mechanisms supplied the institutional response.

An earlier case, *Fruehauf*, although not itself a technical data case, illustrates the same point. In that case, the minority shareholders of a US subsidiary in France applied to the French court for relief against the authority of the U.S.-controlled management or shareholders which planned to observe the U.S. embargo against supplying tractors to China.[55] The French court's intervention in the governance of the French subsidiary was initiated by minority shareholders and resolved through domestic corporate law. The court did not frame the case primarily as one of public international law or national policy. As Lowenfeld observed, "[t]he Court of Appeal seems not to address the concerns of national policy … but for the most part treats the case as a problem in corporate law."[56] Yet private international law was implicit in the result. The French subsidiary was likely subject to French company law under the applicable French choice-of-law rules for corporate matters, and the French court assumed jurisdiction over the French company under its rules of judicial jurisdiction. Although these conflicts aspects may not have been emphasized by commentators, they were what allowed domestic private law to determine the practical effect of U.S. extraterritorial policy.

Similarly, in the aforementioned Dutch case during the Siberian Pipeline crisis, the Dutch court's conclusion that the June 22 Measures were contrary to public international law mattered because it affected the availability of a private-law defence under Dutch law.[57] Thus, these examples show that private international law can complement public international law in resisting extraterritoriality. In short, private defensive mechanisms became effective because private international law supplied the forum, the applicable law, and practical enforcement.

3. The Untested Private-Law Component of U.S. Data Extraterritoriality

One aspect of the Siberian Pipeline dispute has received less attention but is especially important for understanding future extraterritorial data regulation: the use of submission clauses to support extraterritorial control. For present purposes, a submission clause refers to a contractual undertaking by a foreign recipient or licensee of U.S.-origin technical data to comply with U.S. export-control regulations, including later amendments to those regulations. This mechanism is significant because it did not rely solely on direct public enforcement. It also sought to make foreign parties comply with U.S. regulatory policy through private contractual undertakings.

---

[55] For details of the Fruehauf case, see Andreas F. Lowenfeld, *International Litigation and the Quest for Reasonableness: Essays in Private International Law* 973–976 (Clarendon Press 1996).

[56] *Id*.

[57] *See supra* note 50.

As noted above, the June 22 Measures applied not only to foreign subsidiaries of U.S. companies, but also to European licensees that had voluntarily submitted to U.S. export-control law. For example, Alsthom had reportedly included in its license the following clause: "Alsthom further undertakes to keep itself fully informed of the regulations (including amendments and changes thereto) and agrees to comply therewith."[58] Thus, even if Alsthom had not specifically agreed at the time of contracting not to re-export the relevant technical data to the Soviet Union, the clause could be read as incorporating later amendments to U.S. export-control regulations, including the June 22 Measures.

The EEC did address this aspect of the June 22 Measures, but only briefly. It objected that "private agreements should not be used in this way as instruments of foreign policy."[59] The broader passage made clear that the EEC regarded submission clauses as an attempt to circumvent the limits imposed by public international law on national jurisdiction. It stated that it was "reprehensible" for U.S. regulations to encourage non-U.S. companies to submit "voluntarily" to mobilization for U.S. purposes, and that where a government systematically encourages the inclusion of such clauses in private contracts, "freedom of contract is misused in order to circumvent the limits imposed on national jurisdiction by international law."[60]

Private international law is embedded in this contractual mechanism. The relevant export-control restriction operates not merely as a standalone public regulation, but as a term incorporated into a private license or transfer agreement. Whether that incorporation is valid depends on the governing law of the contract. The governing law, in turn, depends on the choice-of-law rules of the forum. The ability to enforce the undertaking depends on jurisdictional rules, available remedies, public policy limits, and any applicable blocking statutes. In other words, the submission clause mechanism works only because private international law supplies the framework through which the contractual obligation is characterized, governed, litigated, and enforced.

The EEC regarded submission clauses as inconsistent with public international law, but its objection was asserted rather than fully developed. The relevant passage appeared outside the EEC's main discussion of the recognized bases of legislative jurisdiction, such as territoriality, nationality, the protective principle, and the effects doctrine. Moreover, the EEC's comments focused principally on the regulation of European subsidiaries of U.S. companies and on the claim that U.S.-origin technical data could itself provide a basis for jurisdiction.[61] The submission clause mechanism therefore remained largely untested as a matter of public international law.

This underexplored feature of the Siberian Pipeline dispute is important because it points toward a potentially more effective form of extraterritorial data regulation. Submission clauses may allow states to pursue extraterritorial regulatory objectives in a form that is less visibly an exercise of direct public legislative jurisdiction, and thus public international law objection. They may operate alone or in combination with public enforcement. Either way, they shift the legal analysis from the simple question whether a state may directly regulate foreign conduct

---

[58] *See supra* note 27.

[59] *Id*. at 204.

[60] Such submission clauses had long been used in U.S. export-control practice. Even before the Siberian Pipeline dispute, 15 C.F.R. § 379.4 imposed a requirement that recipients or importers of regulated technical data provide written assurances against re-export to sanctioned countries, thereby binding foreign recipients of U.S.-origin technical data to U.S. regulatory restrictions through contractual undertakings rather than only through direct public regulation.

[61] *See* Lowe, *supra* note 27, at 218.

to the more complex question whether foreign parties may be required to accept regulatory obligations through private law instruments.

Modern regulatory practice in the United States, the European Union, and China reflects these lessons, both offensively and defensively. Their respective approaches are discussed below.

IV. Neo-Extraterritoriality in Data Law Through Private International Law

Modern data regulation has absorbed these lessons. Rather than relying only on direct public enforcement against foreign actors, contemporary data regimes increasingly operate through a hybrid model. Public law continues to define the regulatory objectives and outer statutory obligations, but private international law supplies many of the mechanisms through which those obligations are implemented, enforced, resisted, or limited. This is especially visible in cross-border data regulation, where states seek to control not only the transfer of data out of their territory, but also the subsequent use, access, processing, and onward transfer of data abroad.

Four features are particularly important. First, states increasingly use submission clauses to regulate foreign data intermediaries and recipients through contract. These measures primarily govern the transfer of data across borders and are referred to in this article as GIVE regulation. Second, they empower data subjects or private parties to enforce data rights, thereby converting public regulatory standards into private claims and potentially enforceable private rights. This technique is found not only in GIVE regulation, but also in laws governing the subsequent use of data, referred to in this article as USE regulation. Third, some regimes compel intermediaries to produce or disclose data located abroad, thereby extending their regulatory reach beyond national borders. These laws are referred to in this article as TAKE regulation. Because such measures are particularly susceptible to conflicts with foreign sovereign authority, some jurisdictions incorporate self-limiting safeguards, including restrictions based on judicial jurisdiction and comity defence, using private international law concepts to reduce the appearance or intensity of public international law conflict. Fourth, states increasingly rely on defensive mechanisms, including blocking statutes, data localisation, and administrative approval requirements, to resist foreign claims to data. These measures are referred to in this article as DEFENSE regulation.

These four features correspond to the lessons of the Siberian Pipeline case. Submission clauses and private enforcement reduce reliance on direct public enforcement and therefore lower the visibility of public international law conflicts. Judicial jurisdiction and comity defence provide a limiting device where the underlying assertion of regulatory power is especially aggressive, as in TAKE statutes that seek access to data held beyond the regulating state's territory. Blocking statutes and data localisation reflect the defensive side of the same dynamic: where foreign data regulation is perceived as excessive, states respond by using domestic law to block, localise, or condition access to data.

The result is not the displacement of public international law. Public international law remains relevant as a source of limits and objections. But the operational mechanism of modern data extraterritoriality increasingly lies elsewhere. It lies in private international law: in contractual submission, private enforcement, forum selection, data-subject jurisdiction, public policy exceptions, arbitration, blocking statutes, and judgment enforcement. This is the central dynamic of hybrid extraterritoriality in data regulation.

A. Feature 1 – The Growing Trend in the Use of Submission Clauses

1. Submission Clauses under GDPR

Despite the EEC's criticism of the use of submission clauses in the Siberian Pipeline case it is perhaps surprising that the EU became the first major jurisdiction to make expansive use of submission clauses in cross-border data regulation.[62] This development began in the 1990s under Directive 95/46/EC, the Data Protection Directive, and continued under the GDPR. The irony is not merely rhetorical. As Basedow observes in a comparable context, the EU's use of a device that it had previously criticised when employed by others is "not without irony."[63]

The GDPR is an EU regulation designed to protect the fundamental rights of data subjects in relation to the processing of personal data.[64] It regulates both the use and the transfer of personal data. With respect to the use of data, it requires that any "processing", a concept defined broadly by the Regulation,[65] must satisfy one of the lawful bases set out in Article 6 and comply with the data protection principles contained in Article 5. Compliance is enforced primarily through public mechanisms, including substantial administrative fines imposed by supervisory authorities.[66] However, this is supplemented by private enforcement.

The GDPR further seeks to protect EU personal data after it leaves the Union by restricting transfers of personal data to third countries.[67] Under the GDPR, as under the Data Protection Directive, transfers of personal data to non-EU countries are subject to restrictions. Such transfers may take place where the European Commission has determined that the third country, territory, sector, or international organisation ensures an adequate level of protection.[68] Alternatively, in the absence of an adequacy decision, the exporting and importing parties may incorporate standard contractual clauses, or SCCs, into their data transfer agreement. The function of the SCCs is to "compensate for the lack of data protection" in the importing country.[69] In other words, where the third country's legal system does not itself provide an adequate level of protection, the contractual mechanism supplies, at least in formal terms, the missing regulatory protection.[70]

A practical illustration may be found in Oracle's Supplier Data Processing Agreement. Oracle incorporates the 2021 SCCs into its supplier agreement, expressly choosing Ireland as the governing law under Clause 17 and the Irish courts as the forum under Clause 18.[71] A European data subject whose personal data is transferred pursuant to the agreement may therefore invoke

---

[62] *See supra* notes 35 and accompanying text.

[63] For the extraterritoriality of the Data Protection Directive generally, see *Sybil Article on DPD Extraterritoriality*, https://www.sybil.es/sybil/article/view/1439. On the EU's use of submission clauses generally, *see* Jürgen Basedow, *Bail-in and International Contract Law: Some Conflict-of-Laws Perspectives on the European Banking Union*, at 258 (observing, in the context of European bank resolution, that "[t]he fact that the EU is now, in relation to bank resolution, making use of a device that it had itself criticized as being inconsistent with international law when employed by other countries in other contexts is not without irony").

[64] GDPR pr GDPR, Preamble 1; Art 1(1)&(2).

[65] W. Gregory Voss, *An American's Guide to the GDPR*, 98 Denv. L. Rev. 93, 144 (2020).

[66] GDPR, art. 83 and 84.

[67] *Id.* Chapter V.

[68] *Id.* art. 45.

[69] *Id.* recital 108 (noting that the SCCs are intended to "compensate for the lack of data protection" in the importing country).

[70] *Id*. art. 46(3)(a). The use of contractual terms to compensate for inadequate data protection in the importing country is not new. It can be traced to earlier German debates on whether contractual arrangements could provide equivalent protection in cross-border data transfer cases. *See* Thomas Hoeren, *Electronic Data Interchange: The Perspectives of Private International Law and Data Protection*, 1 L. Comput. & Artificial Intelligence 327, 329 (1992).

[71] *See* Oracle Corp., *Supplier Data Processing Agreement (SDPA-P)* app. 2, § 4(a)–(b), at 15 (July 7, 2025).

the third-party beneficiary provisions of the SCCs before the Irish courts, notwithstanding that the data subject is not a party to the contract.

The SCCs are, in effect, a form of submission clause. Their contractual character was confirmed by the CJEU in *Schrems II*, where the Court described them as "inherently contractual" in nature.[72] This is important because their regulatory effect depends precisely on their contractual form. They do not directly subject every foreign recipient to the GDPR as a matter of statutory application. Rather, they require the foreign importer to accept GDPR-like obligations as a matter of contract.

The SCCs have extraterritorial effect because foreign data importers are restricted in their onward transfers of data. They may re-export the data only to countries that provide the required level of protection, or they must impose equivalent obligations by incorporating the SCCs into their own contracts with further recipients. The SCCs require data importers to comply with a range of contractual obligations designed to protect personal data. These obligations mimic many of the statutory requirements imposed by the GDPR on controllers and processors directly subject to the Regulation, including principles of transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.[73] These principles are all reproduced in the SCCs.[74]

The purpose of the SCCs is to cover data importers who are not otherwise subject to the territorial jurisdiction of the EU. This point is important. The SCC regime is a contractual mechanism designed to extend GDPR-like standards to recipients located outside the EU and outside the GDPR's direct territorial reach. The Commission's own Q&A illustrates this. In the Module 4 example, SCCs may be used where a Luxembourg company transfers data from its server in Luxembourg back to a Moroccan client. That example is significant because it shows that the SCCs are designed to reach a recipient who is not otherwise directly subject to the GDPR.[75]

The SCCs remain an important route for data transfers out of the EU because most countries have not received an adequacy decision, including the United States. Instead of directly prohibiting transfers by foreign intermediaries to countries with substandard data protection regimes, the EU uses contractual obligations to project its regulatory standards beyond its territory. This avoids, or at least reduces, public international law scrutiny. Indeed, although the GDPR is widely known for its extraterritorial reach, discussions of GDPR extraterritoriality usually focus on Article 3 (to be discussed below), rather than the SCCs. The SCCs, as

---

[72] Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 132 (July 16, 2020) (describing the SCCs as "inherently contractual" in nature).

[73] Voss, *supra* note 66, at 112. These principles are all reproduced in the SCCs.

[74] GDPR art. 5 (setting out the seven data protection principles). These are all reproduced in Commission Implementing Decision (EU) 2021/914, of 4 June 2021, on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679, 2021 O.J. (L 199) 31 [hereinafter SCCs 2021], cl. 2(a).

[75] *See* Eur. Comm'n, *New Standard Contractual Clauses — Questions and Answers Overview*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (last visited May 16, 2026); *see also* Pietro Franzina, *Standard Contractual Clauses and Private International Law: Welcome Clarifications and Lingering Doubts in the Light of the EU Commission's Q&As*, EAPIL (Aug. 8, 2022) ("SCCs are, by definition, incorporated within an international contract between a controller/processor of personal data established in the EU (or subject to the GDPR pursuant to Article 3(2) thereof) and a controller/processor established in a third country and placed beyond the scope of application of the GDPR (cf Q&A No. 24)."). Note also that GDPR, art. 46(3)(a) refers expressly to "recipient" in addition to controller and processor, whereas Article 3 of the GDPR applies generally only to controllers and processors. Note also that Art. 46(3)(a) expressly referred to "recipient" of data in addition to controller and processor, and GDPR generally only applies to controller and processor under Art. 3.

submission clauses, have therefore largely escaped sustained scrutiny as an extraterritorial regulatory mechanism.[76]

The SCCs are also better designed than the submission clauses at issue in the Siberian Pipeline case. First, they avoid the "Trojan horse" problem. The EU does not unilaterally change the incorporated contractual obligations after the parties have entered into the agreement. Instead, amendments to the SCC regime are made through replacement of the standard contractual clauses as a whole.[77] In this respect, the SCCs are closer to the incorporation of foreign law as terms of contract, a familiar and generally accepted technique in private international law and commercial drafting.[78]

Second, the SCCs provide governing law and jurisdiction clauses, thereby increasing certainty. That said, it remains unclear whether the governing law clause in the SCCs fully complies with the Rome I Regulation's requirement of a free choice of law. [79] In Modules 2 and 3, the parties' freedom is limited because they must generally choose the law of the Member State in which the data exporter is established, unless that law does not permit third-party beneficiary rights. This creates an unresolved private international law issue.[80]

If the chosen law is not regarded as a valid choice under Rome I, the applicable law would have to be determined through the ordinary choice-of-law rules, such as characteristic performance or closest connection. In many cases, that analysis may still lead to the law of an EU Member State, for example the law of the exporter's establishment or possibly the law connected with the data subject. Alternatively, the SCCs may be characterised as giving effect to mandatory EU data protection law, in which case the ordinary Rome I analysis may be displaced or substantially qualified.[81]

---

[76] *See* Voss, *supra* note 66, at 113; *see also* Anu Bradford, *The GDPR as Global Data Protection Regulation*, Am. J. Int'l L. Unbound, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688 (mentioning the SCCs only in passing, at n.21); Lokke Moerel, *The Long Arm of EU Data Protection Law*, 13 Glob. J. Comp. L. 201 (2024), https://brill.com/view/journals/gjcl/13/2/article-p201_004.xml (containing no discussion of the SCCs).

[77] *See* Eur. Comm'n, *supra* note 76, at Q. 20 (noting that changes in terms set out in the SCCs are effected by a wholesale change of the set). The "Trojan horse" critique, associated with Lowe, refers to the concern that a state could bind foreign parties to regulations that it subsequently amends unilaterally, thereby concealing an expansionary regulatory agenda within a private contract. *See* Lowe, *supra* note 35, at 525–27.

[78] Lowe, a prominent critic of the submission clause, himself accepted that such incorporation by reference would be "unexceptionable" where the parties use external legal materials as a shorthand method for expressing the terms of their agreement. The problem in the Siberian Pipeline case, on his view, was not incorporation as such, but the use of contract as a vehicle for foreign public regulation, *see* Lowe, *supra* note 35, at 524 ("It is clear that the references in the contracts to the US export regulations [in the context of the Siberian Pipeline case] were not a shorthand method for expressing the actual terms of the parties' agreement, such as is commonly the case where, for example, the provisions of the Carriage of Goods by Sea Act are incorporated by reference into the contracts. Such an incorporation would be unexceptionable.").

[79] Regulation (EC) No 593/2008, of the European Parliament and of the Council of 17 June 2008, on the Law Applicable to Contractual Obligations (Rome I), 2008 O.J. (L 177) 6 [hereinafter Rome I], art. 3 (requiring that a choice of law be "free"). *See* Giuliano-Lagarde Report, 1980 O.J. (C 282) 1, at 15.

[80] Franzina, *supra* note 76.

[81] Rome I art. 4(2) (characteristic performance as default rule); *id.* art. 4(4) (closest-connection escape). Alternatively, GDPR obligations may qualify as *lois de police* under Rome I art. 9(2), applicable regardless of the governing law.

2. *Submission Clauses under Chinese Data Law*

China's personal information protection regime borrows extensively from the GDPR.[82] This includes the use of SCCs for the outbound transfer of personal information.[83] Similar to the GDPR SCCs, the Chinese SCCs incorporate substantive obligations under Chinese personal information protection law into the contractual relationship between the domestic personal information handler and the overseas recipient. Clause 3 of the Chinese SCCs reflects many of the core principles and obligations set out in the Personal Information Protection Law ("PIPL"), including legality, legitimacy, necessity, transparency, purpose limitation, data minimisation, accuracy, security, and protection of individual rights.[84] In this sense, the Chinese SCCs also operate as submission clauses: they require the foreign importer to accept Chinese data protection standards as contractual obligations.

The Chinese SCCs also regulate onward transfers. The overseas recipient must ensure that any onward transfer to a third party is subject to conditions that preserve the level of protection required by Chinese law.[85] This mirrors the logic of the GDPR SCCs. The initial transfer serves as the contractual entry point, but the contract then extends regulatory control downstream.

For present purposes, however, the Chinese SCCs differ from the EU SCCs in two important respects. First, the Chinese SCC route is more limited in regulatory scope. Data can only be transferred under Chinese SCCs to the extent that (i) the Chinese personal information handlers are not critical information infrastructure operators; (ii) they did not exceed the relevant volume thresholds for personal information; or (iii) the data being transferred are not sensitive personal information.[86] These excluded data exports are subject to security assessment or other regulatory scrutiny by the relevant Chinese authorities.[87]

This shows that China's SCC mechanism is only one part of a more state-centred data export regime. For lower-risk transfers, China uses the private-law technique of standard contracts. For higher-risk transfers, especially those involving critical infrastructure or bulk/sensitive data, it retains direct administrative scrutiny and approval.

Second, the Chinese SCCs differ from the EU SCCs in their dispute-resolution design. Chinese law also provides for private enforcement by data subjects as third-party beneficiaries against the contracting parties for breach of the SCCs.[88] However, where a data subject exercises third-party beneficiary rights, the Chinese SCCs permit more flexibility by generally allowing the data subject to choose the applicable law, and the parties agree that such choice shall be followed.[89]

For disputes between the personal information handler and the overseas recipient, the governing law is Chinese law, but the parties may choose either litigation before Chinese courts

---

[82] Zhang Zhe & Qi Aimin, *On the Construction of Extraterritorial Effect System of Personal Information Protection Law in China*, J. Chongqing U. (Soc. Sci. Ed.), no. 5, 2022, at 207, 215.

[83] Measures for the Standard Contract for the Cross-Border Transfer of Personal Information (issued by the Cyberspace Admin. of China, Feb. 22, 2023, effective June 1, 2023) [hereinafter Chinese SCCs].

[84] *See* Chinese SCCs cl. 3 (reflecting the principles set out in arts. 4–11 of the Personal Information Protection Law of the People's Republic of China [hereinafter PIPL]).

[85] *See* Chinese SCCs cl. 3(8)(4).

[86] *See* Chinese SCCs art. 1; *see also* Ning Xuanfeng et al., *Comparative Analysis of China SCC and GDPR SCC*, King & Wood Mallesons (July 19, 2022), https://www.kingandwood.com/cn/en/insights/latest-thinking/comparative-analysis-of-china-scc-and-gdpr-scc.html.

[87] *See id.* art. 1; Cybersecurity Law of the People's Republic of China art. 39 (2017); PIPL art. 40.

[88] *Id.* art. 5(5).

[89] *Id.* art. 4.

or arbitration.[90] This gives the contracting parties greater dispute-resolution flexibility than the EU SCCs, especially because arbitration may provide a more internationally portable enforcement mechanism through the New York Convention. At the same time, the availability of arbitration further confirms the broader point of this section: submission clauses do not merely incorporate substantive regulatory standards. They also use private international law mechanisms, including governing law, jurisdiction, arbitration, and third-party beneficiary rights, to make those standards operational beyond the territory of the regulating state.[91]

The Chinese model is therefore hybrid in a different way from the GDPR. It borrows the EU's contractual technique, but embeds it within a more state-centred structure in which lower-risk transfers may proceed through standard contracts, while higher-risk transfers remain subject to administrative control. It also appears to give more teeth to private enforcement. Together, it is a stricter scheme than EU on GIVE regulation, even though they both adopt submission clauses as a private mechanism.

3. Submission Clauses under US EO 14117

The United States has also adopted a form of submission clause in the recent Executive Order 14117 (hereinafter "EO 14117").[92] Under the EO 14117 and the implementing framework, foreign importers of data may be required to agree contractually with U.S. exporters that they will not re-export the relevant data to six countries of concern, including China and Russia.[93] This gives EO 14117 the same basic extraterritorial structure: foreign intermediaries are regulated through contractual commitments imposed at the point of export.

EO 14117, however, differs from the GDPR and the Chinese model in three important respects. First, while the GDPR and the Chinese equivalent seek to regulate not only the "GIVE" of data but also the "USE" of data (to be discussed below), EO 14117 is closer to an old-fashioned data embargo. It focuses on preventing transfers of data to countries of concern. It is therefore more directly a "GIVE" statute. Because of this, it is more severe and may require stronger justification.

Second, unlike the GDPR and its Chinese counterpart, EO 14117 does not prescribe a complete set of standard contractual terms. Instead, it simply requires contractual restrictions with the effect of prohibiting onward transfers to countries of concern or covered persons. The U.S. Department of Justice ("DOJ") provides sample clauses, but the guidance makes clear that the language is only an example. U.S. persons are expected to craft clauses that satisfy the regulatory requirements and make sense for their own transactions and business operations. The U.S. approach is therefore less standardised and leaves more room for private ordering.[94]

---

[90] *Id.* art. 9.

[91] Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 38. As of 2024, the Convention has 172 contracting states, making an arbitral award significantly more portable than a foreign court judgment.

[92] Exec. Order No. 14,117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15,421 (Feb. 28, 2024), https://www.presidency.ucsb.edu/documents/executive-order-14117-preventing-access-americans-bulk-sensitive-personal-data-and-united.

[93] The six countries of concern designated under EO 14117 and implementing regulations are China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. *See* 28 C.F.R. § 202.1 (2024).

[94] *See* U.S. Dep't of Just., *Compliance Guide: Data Security Program*, at 6 (2025), https://www.justice.gov/opa/media/1396356/dl (providing sample contractual language and noting that "[t]his language is just an example" and that "U.S. persons should craft language that satisfies the DSP's requirements and that makes sense for their transactions and business operations").

Third, unlike the SCCs, EO 14117 may require parties to revisit existing contractual arrangements. DOJ guidance recognises that compliance may require regulated parties to identify data flows, revise internal policies, change vendors or suppliers, implement new security requirements, and revise existing contracts. Given this retrospective nature, EO 14117 is potentially more disruptive than the GDPR SCC regime.[95]

A further difference concerns enforcement. The GDPR SCCs expressly contemplate enforcement by data subjects as third-party beneficiaries. EO 14117 does not create an equivalent private enforcement role for data subjects. This is understandable because a data subject's individual right is not necessarily violated merely because data is transferred to one of the six countries of concern. But this also means that enforcement of EO 14117 submission clauses is likely to arise in a different way. The U.S. exporter may seek to enforce the contractual restriction only after facing regulatory consequences from the U.S. government, or may invoke the clause as a defence to a claim for breach of its own data transfer obligations.[96]

Across these three jurisdictions, the use of submission clauses has been successful in avoiding public international law scrutiny. Although the GDPR is widely recognised as extraterritorial, that discussion rarely centres on the SCCs. The same is true of the Chinese standard contract mechanism. As for EO 14117, there appears to have been little allegation so far that its contractual mechanism has an extraterritorial character. The extraterritoriality of submission clauses has therefore largely flown under the radar.

4. Are Submission Clauses Compatible with Public International Law?

There is a question of whether submission clauses comply with public international law. After the Siberian Pipeline case, some commentators argued that submission clauses could not bypass public international law. Lowe, for example, argued that public and private international law each has its own domain, and that a state cannot use a submission clause to regulate public law matters indirectly. On this view, the contractual form of the clause cannot conceal its public regulatory function. Lowe's most vivid criticism was that submission clauses provide "the saddle for public laws to ride on the backs of private contracts." To assess such clauses only by private international law rules would therefore, in his view, commit a category mistake,[97] leading to an "indirect enforcement of the prerogative right of a foreign State."[98]

This objection is powerful, but it adopts too narrow a view of the relationship between public and private international law. The boundary between the two disciplines has never been entirely clear. Lowe himself acknowledged that it is "difficult to draw a satisfactory boundary between public and private laws."[99] More importantly, in practice, states ordinarily respect party autonomy not only in the familiar forum selection agreements and choice-of-law agreements, but also in the parties' decision to incorporate foreign regulatory standards into their contracts.

---

[95] U.S. Dep't of Just., Nat'l Sec. Div., *Implementation and Enforcement Policies for the Data Security Program*, at 2 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396346/dl?inline.

[96] EO 14117 is principally concerned with national security—preventing countries of concern from accessing bulk sensitive data about U.S. persons—rather than with protecting individual data subjects' rights in particular transfers. *See* Exec. Order No. 14,117 pmbl.

[97] Lowe, *supra* note 35, at 525.

[98] F.A. Mann, *Prerogative Rights of Foreign States and the Conflict of Laws*, *in* Studies in International Law 492 (1973), *cited in* Lowe, *supra* note 35, at 525.

[99] Lowe, *supra* note 35, at 526 ("First, there is the question of classification. It must be admitted that it is difficult to draw a satisfactory boundary between public and private laws.").

English case law illustrates this point. In *Regazzoni v K.C. Sethia*, the House of Lords refused to enforce a contract that was intentionally designed to violate Indian export control law prohibiting the sale of jute to South Africa.[100] Lord Reid emphasised that the issue was not strictly one of international law, but one of English public policy.[101] The English court therefore treated the effect of foreign export control law as a matter for domestic private law, informed by international law and comity, rather than as an automatic prohibition derived from public international law.[102]

This suggests that a state should have autonomy to decide whether to give effect to such contractual arrangements. A state may certainly prohibit such contracts through domestic law, including blocking statutes. But that is different from saying that public international law imposes a wholesale prohibition on submission clauses. F.A. Mann made the point more directly. In his view, an American supplier may, by contractual term, bind foreign buyers to observe American law generally and export restrictions in particular. For Mann, this point was "obvious to any private international lawyer."[103] Whether such a contractual term is effective therefore depends on the proper law of the contract, subject to any overriding legislation, such as a blocking statute. On this view, submission clauses are not inherently unlawful or objectionable. They are, in principle, legitimate contractual devices.

This view has also been supported by Ryngaert, who criticises Lowe's position and argues that there is no rule of international law prohibiting private parties from "bonding" to a higher regulatory standard. That position is more consistent with modern regulatory practice. International contracts routinely incorporate standards derived from foreign regulatory regimes, including sanctions, export controls, anti-corruption rules, human rights obligations, environmental standards, and data protection requirements.[104]

Other commentators object that parties should not be able to create legislative jurisdiction by contract. They rely by analogy on the rule that parties cannot confer subject matter jurisdiction by consent.[105] That objection is unpersuasive. The fact that a choice may not always be given effect does not mean that the choice can never be made. Forum selection clauses and choice-of-law clauses work precisely in this way. They do not bind courts absolutely, but they create a private-law choice that courts may recognise subject to limits. Moreover, subject matter

---

[100] *Regazzoni v. K.C. Sethia (1944) Ltd*., [1958] A.C. 301, 323 (HL).

[101] *Id.*

[102] Lowe argued to the contrary without referring to *Regazzoni*. *See* Lowe, *supra* note 35, at 525 ("Thus, if the question of the effect of a submission clause arose in private litigation — for example, in municipal proceedings where a prohibition under the export regulations was pleaded as a defense to a claim arising from a failure to perform a contract for the re-exportation of US technology . . . a municipal court . . . would be likely to frame its decision in terms of private international law rules prohibiting the enforcement of foreign public law.").

[103] F.A. Mann, *Further Studies in International Law* 62–63 (1990) ("Indeed by a contractual term requiring buyers to observe American law in general and export restrictions in particular the American supplier can bind buyers who are complete strangers. This will be obvious to any private international lawyer . . . . [The validity of a submission clause] depends on the proper law, and if the proper law is that of the United States [the clause is valid], except in cases in which the buyer's sovereign makes specific provision under such legislation as the Protection of Trading Interests Act 1980 . . . . [N]either method is contrary to law or can properly be described as 'objectionable' . . . . It is in law perfectly legitimate.").

[104] Cedric Ryngaert, *Jurisdiction in International Law: United States and European Perspectives* 456 (2007) (unpublished Ph.D. dissertation, Katholieke Universiteit Leuven), https://lirias.kuleuven.be/retrieve/67311 (calling Lowe's view misconceived and stating that "there is no rule of international law which prohibits private parties from 'bonding' to higher regulatory standard").

[105] Note, *Extraterritorial Application of the Export Administration Act of 1979 Under International and American Law*, 81 Mich. L. Rev. 1308, 1326 (1983) ("Under those principles, the 'parties cannot waive lack of [subject matter] jurisdiction by express consent, by conduct, or even by estoppel.' The rationale behind this rule is that jurisdictional concerns are too fundamental in our federal system to be left to the 'whims' of the litigants.").

jurisdiction is a domestic constitutional limitation, particularly in U.S. law. It is not, without more, a rule of public international law.

A further objection is that submission clauses undermine party autonomy because the foreign party's consent is not truly voluntary.[106] However, commercial parties to international contracts routinely negotiate against the background of regulatory constraints. Export controls, sanctions, licensing requirements, data protection rules, financial regulations, and mandatory compliance terms all affect contractual bargaining. A submission clause is one such constraint. A party remains free not to enter into the contract if the regulatory terms are commercially unacceptable.

In summary, submission clauses do more than reduce the visibility of public international law issues. They should also withstand public international law scrutiny. Private party consent provides an additional basis for regulatory projection, alongside the traditional justifications under public international law. If there was doubt in the 1980s, modern practice in data regulation shows a significant shift toward acceptance. Submission clauses have also been used in other regulatory contexts, including EU bail-in clauses.

5. Private International Law Limits on the Effectiveness of Submission Clauses

The more difficult question is not whether submission clauses are categorically impermissible, but how effective they are in achieving their regulatory purpose. Their effectiveness depends on the private international law rules of the relevant forum. As Basedow observes, even if the public international law question is put aside, third-country courts may still decline to honour such clauses for private international law reasons.[107] These will include all three aspects of private international law:

1. Where may a party sue for breach of the submission clause? This is a question of judicial jurisdiction.
2. Which law governs the breach of contract claim? This is a question of choice of law.
3. Will a judgment obtained on the contractual claim be recognised and enforced abroad?[108]

Foreign states may resist submission clauses through ordinary private international law techniques. A court may decline jurisdiction on forum non conveniens grounds. It may refuse to apply the chosen law on public policy grounds or because of overriding mandatory rules. It may also refuse recognition or enforcement of a judgment if enforcement would violate public policy.

This is where blocking statutes remain important. Foreign states may also use the extraterritorial purpose of a submission clause as a reason to resist jurisdiction, refuse the chosen law, or deny enforcement. Professor Basedow therefore expect submission clauses to have only a "limited effect." In particular, courts may consider such clauses as requiring the

---

[106] *Id.*

[107] Basedow, *supra* note 64, at 258 ("Irrespective of the public international law question, however, it cannot be ruled out that third-country courts will, despite a [submission clause], decline to honor a [public law purpose] for reasons of private international law.").

[108] *See supra* Section II.C (discussing the relationship between public and private international law).

application of foreign public law, which many jurisdictions have traditionally been reluctant to enforce.[109]

That said, the picture is not entirely pessimistic. In the United States, for example, an EU data exporter or a data subject with third-party beneficiary status under the SCCs may be able to sue a U.S. data importer to enforce the clauses in a U.S. court. This illustrates the value of the SCC structure. It is not merely a regulatory command; it is a contract with an identifiable claimant, an identifiable defendant, and an enforceable set of obligations.[110]

Beyond this, submission contracts should generally be treated like other contracts under private international law. For Modules 1 to 3 of the SCCs, the parties must choose the law of an EU Member State that recognises third-party beneficiary rights.[111] This facilitates enforcement by data subjects. For Module 4, where the connection with the EU is likely to be more remote, the parties may choose any law that recognises third-party beneficiary rights, including non-EU law. As for jurisdiction, Modules 1 to 3 require the selection of an EU Member State court, while Module 4 permits selection of a non-EU court. China similarly requires Chinese law for disputes between the contracting parties, while allowing them to choose either Chinese courts or arbitration.[112]

By contrast, the EO 14117 sample clauses do not contain forum selection or governing law clauses. This is sensible because EO 14117 does not contemplate enforcement by data subjects. The data importer and exporter are likely to be sophisticated parties capable of selecting a commercially appropriate forum and governing law. However, an intentionally ineffective choice of forum or law may be treated by the DOJ as evidence of failure to comply with EO 14117.

As to enforcement abroad, a judgment based on a submission clause should generally be enforceable unless the submission contract is blocked by a blocking statute or contrary to the public policy of the enforcing forum. The same considerations that arise at the choice-of-law stage may therefore arise again at the recognition and enforcement stage.

Overall, even though submission clauses do not guarantee effective enforcement, they remain superior to traditional extraterritorial public enforcement. Direct public enforcement carries the stigma of public international law violation. Even if the regulating state can withstand diplomatic pressure, it will often be difficult to bring a public enforcement action in a foreign court or to have a resulting judgment enforced abroad. Private international law does not provide a perfect solution, but it provides a useful alternative. It allows states to project regulatory standards through contracts, private claims, chosen law, selected courts, arbitration, and ordinary judgment enforcement mechanisms. This is a central feature of hybrid extraterritoriality in data regulation.

---

[109] Basedow, *supra* note 64, at 258 ("[O]n the whole one can expect [submission clauses] to have only a limited effect.").

[110] *See* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 22 Sedona Conf. J. 1, 342 (2021), https://www.thesedonaconference.org/download-publication?fid=5883 ("An EU data exporter with whom the U.S. organization has executed the standard contractual clauses, or a data subject with status as a third-party beneficiary under those clauses, could bring an action to enforce the clauses against the U.S. organization in a U.S. court.").

[111] Commission Implementing Decision (EU) 2021/914, of 4 June 2021, on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679, annex, cl. 17, 2021 O.J. (L 199) 31 [hereinafter SCCs 2021].

[112] Chinese SCCs art. 9.

B. Feature 2 – Creation of Private Enforcement Rights by Data Subjects for More Effective Enforcement Under Private International Law

Although submission contracts bring many benefits, the regulation of foreign data activities cannot depend entirely on contract. Many such activities are not based on a consensual relationship. This is particularly true where the regulation does not merely seek to control the GIVE of data, but also seeks to regulate the USE of data after collection, access, transfer, or processing. The second feature of modern hybrid regulation is therefore the creation of private enforcement rights for data subjects. As discussed above, this feature complements submission clauses, but it also extends beyond the GIVE to the USE of data. Together, submission clauses and private enforcement make extraterritorial data regulation more effective through private international law.

This second feature is most notable in the GDPR. In its extraterritorial application, the GDPR is mainly a USE statute. Its principal purpose is not to prevent foreign controllers or processors from obtaining personal data as such, but to regulate how personal data are processed. The GDPR defines "processing" broadly as "any operation or set of operations which is performed on personal data or on sets of personal data," including "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[113]

The GDPR has an explicit and broad extraterritorial reach. Under Article 3(1), the GDPR applies, first, to foreign controllers or processors with an establishment in the EU where the processing is carried out "in the context of the activities" of that establishment, "regardless of whether the processing takes place in the Union or not."[114] Under Article 3(2), it also applies to controllers or processors without such an EU establishment where their processing activities relate to "the offering of goods or services" to data subjects in the Union, irrespective of payment, or to "the monitoring of their behaviour" as far as that behaviour takes place within the Union.[115] Compared with the Siberian Pipeline case, the scope of the GDPR's extraterritoriality is arguably even broader. Commentators have described the GDPR's extraterritoriality as "expansive," and as "much wider than might be thought."[116]

The establishment approach is similar to the subsidiary approach adopted by the United States in the Siberian Pipeline case. In that case, the United States sought to project its law outward by relying on the relationship between U.S. nationals and foreign subsidiaries. Under the GDPR, by contrast, the EU may project its law outward by relying on the relationship between a foreign controller or processor and its EU establishment. The concept of "establishment" is broad.[117] Recital 22 provides that establishment "implies the effective and real exercise of activity through stable arrangements," and that the legal form of those arrangements, whether "through a branch or a subsidiary with a legal personality," is not determinative.[118]

---

[113] GDPR art. 4(2).

[114] *Id.* art. 3(1).

[115] *Id.* art. 3(2).

[116] *See* The Sedona Conference, *Practical In-House Approaches*, *supra* note 111, at 289 (describing GDPR extraterritoriality as "expansive"); *see also* Lokke Moerel, *The Long Arm of EU Data Protection Law*, 13 Glob. J. Comp. L. 201, 201 (2024) (commenting that the extraterritorial effect of the GDPR is "much wider than might be thought").

[117] *See* Dan Jerker B. Svantesson, The Extraterritoriality of EU Data Privacy Law — Its Theoretical Justification and Its Practical Effect on U.S. Businesses, 50 Stan. J. Int'l L. 53, 84 (2014) (characterising the GDPR's Art. 3(1) as "exploit[ing] the very same establishment device that the US used in the Pipeline controversy, but doing so in a more restrained way").

[118] GDPR recital 22.

For this reason, the establishment approach cannot easily be justified by the nationality principle. Commentators have argued that Article 3(1)'s predecessor, Article 4 of the Data Protection Directive, could be justified by the territoriality principle.[119] However, Article 3(1) added the phrase "regardless of whether the processing takes place in the Union or not." That language makes the GDPR's claim to territoriality more difficult. It does not eliminate the territorial connection altogether, since the processing must still occur "in the context of the activities" of an EU establishment. But it stretches territoriality by treating foreign processing as sufficiently connected to the EU through the activities of a Union establishment.[120]

Article 3(2) raises an even more difficult question. It may be argued that the targeting approach can be justified by the effects doctrine.[121] Yet the latest report on the extraterritorial enforcement of the GDPR commissioned by the European Data Protection Board recognises the difficulty. The report states that reliance on the effects doctrine requires a "substantial effect" within the prescribing state. The GDPR, however, relies on a "targeting" criterion, and "the 'substantial effect' of the conduct is not required." The report therefore concludes that, although arguments may be made in favour of such broad prescriptive jurisdiction, its legitimacy is "at least controversial from the public international law standpoint."[122]

Finally, some commentators have advanced an argument based on the passive personality principle, since the data subjects protected by the GDPR are EU citizens or residents.[123] In particular, emphasis has been placed on the argument that "data protection rises to the level of a fundamental right," thereby making the "EU's exercise of jurisdiction… mandatory."[124] However, the passive personality principle has never been as firmly established as territoriality or nationality.[125] Nor can it yet be said that this formulation of a passive protection principle has received worldwide support as part of customary public international law. Further, to the extent that the foreign controller or processor has not entered into a transfer agreement incorporating the SCCs, the GDPR's extraterritoriality cannot be justified by consent either.

In short, whether the GDPR's extraterritoriality can be fully justified remains controversial. Feature 2 does not solve that problem. Private enforcement does not itself justify extraterritoriality. Its significance lies elsewhere: it assists the enforcement of an otherwise controversial extraterritorial regulatory regime.

Unlike the old model in the Siberian Pipeline case, this extraterritorial application is enforced through a hybrid mechanism combining public and private enforcement. One lesson of the Pipeline case was the difficulty of enforcing public regulation extraterritorially. Similarly, under the GDPR, a foreign controller or processor may be subject to fines and public reprimands if it has a branch, subsidiary, or substantial assets in the EU.[126] But overseas public enforcement will be difficult, if not impossible. The EDPB-commissioned report states that

---

[119] Commentators have argued that Article 3(1)'s predecessor, Article 4 of the Data Protection Directive, could be justified on territorial grounds. *See* Svantesson, *supra* note 118, at 84.

[120] *See* Bradford, *supra* note 77, at 6 (justifying the GDPR's extraterritoriality on the basis of a "territorial extension" principle).

[121] *See* Svantesson, *supra* note 118, at 85 ("The types of extraterritorial claims found in the context of data privacy [under GDPR] seem to fall squarely with the effects doctrine.").

[122] European Data Protection Board, *Report on the Extraterritorial Enforcement of the GDPR*, at 5 (Oct. 2024), https://www.edpb.europa.eu/system/files/2024-10/edpb_20240417_report_extraterritorial_enforcement_gdpr_en.pdf [hereinafter EDPB Report].

[123] *See* Bradford, *supra* note 77, at 6 (advancing an argument under the passive personality principle on the basis that the data subjects protected by the GDPR are EU citizens or residents).

[124] *Id.*; *see also* Svantesson, *supra* note 118, at 84–85.

[125] Svantesson, *id*. at 81; *see also* Mann, *The Doctrine of Jurisdiction*, *supra* note 12.

[126] The Sedona Conference, *Practical In-House Approaches*, *supra* note 111, at 285.

recognition and enforcement of penalty judgments is a "theoretical possibility," but "seems highly unlikely."[127] This is because foreign fines and penal judgments are not normally enforceable. That is certainly the position in U.S. courts.[128]

Our focus is therefore on private enforcement, under which data subjects are empowered to bring litigation against foreign parties for misuse of their data. Under Article 82 of the GDPR, data subjects who have suffered damage as a result of a GDPR infringement have the right to receive compensation from the controller or processor for the damage suffered. Under Article 79(1), they are entitled to an effective judicial remedy where they consider that their rights under the GDPR have been infringed as a result of the processing of their personal data in non-compliance with the Regulation. Article 79(2) provides that data subjects may bring such proceedings before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has habitual residence,[129] unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.[130]

Beyond these primary fora, some commentators further argue that data subjects should be able to bring actions in other Member State courts by relying on general jurisdiction rules, including the Brussels I-bis Regulation, so long as those general rules do not conflict with Article 79.[131] On this view, "GDPR rules supplement but take precedence over the general rules on jurisdiction."[132] The interplay between the GDPR and the Brussels I-bis Regulation has not yet been ruled upon by the CJEU. However, if this interpretation is adopted, the GDPR gives data subjects a wide range of fora within the EU to bring private actions.[133]

A private action based on the right to compensation has many of the private international law advantages highlighted in Feature 1. For example, under U.S. law on the recognition and enforcement of foreign judgments,[134] a judgment obtained by a data subject is generally less likely to be treated as penal because its primary function is compensation. As the Sedona Conference report puts it, such judgments are unlikely to violate the rule against enforcing penal judgments because their "primary purpose is to compensate data subjects," rather than punish the defendant, and because they "do not serve to benefit public authorities."[135]

---

[127] EDPB Report, *supra* note 123, at 28 (stating that recognition and enforcement of penalty judgments is a "theoretical possibility," but "seems highly unlikely").

[128] *See id.* at 26–27; The Sedona Conference, *Practical In-House Approaches*, *supra* note 110, at 300–302. EDPB Report, *supra* note 123, at 28. The report was commissioned by the EDPB to assess the practical enforceability of the GDPR against non-EU controllers and processors and to identify strategies for improving cross-border enforcement cooperation.

[129] This is subject to the exception that the controller or processor is a public authority of a Member State acting in the exercise of its public powers. *See* GDPR, *supra* note 2, art. 79(2).

[130] GDPR art. 79(1)–2; art. 82(1).

[131] Lydia Lundstedt, *International Jurisdiction over Cross-Border Private Enforcement Actions Under the GDPR*, 4 Stockholm Master L.J. 245, 250–53 (2018); *see also* Eduardo Silva de Freitas, *The Interplay of Digital and Legal Frontiers: Analyzing Jurisdictional Rules in GDPR Collective Actions and the Brussels I-bis Regulation*, 2023-13 Nederlands Internationaal Privaatrecht 227, 234 (2023).

[132] *Id.* at 253 ("GDPR rules supplement but take precedence over the general rules on jurisdiction.").

[133] Regulation (EU) No 1215/2012 (Brussels I-bis), 2012 O.J. (L 351) 1. For the pending interplay question, *see* Lundstedt, *supra* note 132, at 250–53; Silva de Freitas, *supra* note 132.

[134] The enforcement of foreign judgments in the United States is generally regarded as a matter of state law. *See* David Epstein et al., *Ristau's International Judicial Assistance* 263 (2d ed. 2014). Most U.S. states have adopted one of two uniform laws: the 1962 Uniform Foreign Money-Judgments Recognition Act [hereinafter UFMJRA] and the Uniform Foreign-Country Money Judgments Recognition Act [hereinafter UFCMJRA]. *See id.* at 264–65. The discussion below is based on those two statutes. For a full discussion of U.S. law on enforcement of GDPR judgments, see The Sedona Conference, *Enforceability of GDPR-Based Compensation Judgments in the United States*, at 1 (2021) [hereinafter Sedona, *Enforceability of GDPR*].

[135] Sedona, *Enforceability of GDPR*, *supra* note 135, at 312.

In the common law tradition, once a judgment is made, the cause of action merges into a judgment debt.[136] A GDPR compensation judgment may therefore resemble an ordinary private judgment arising from a contractual or tortious claim. Of course, a foreign court may still resist enforcement on the basis of public policy, overriding mandatory law, a blocking statute, or by tracing the judgment back to the GDPR as a public law regulation and characterising it as penal.[137] In addition, although private enforcement may allow courts to grant non-monetary remedies such as injunctions, such remedies are generally less portable because many jurisdictions enforce only foreign monetary judgments.[138]

The more intriguing issue is whether a private GDPR judgment satisfies the jurisdictional requirement under U.S. enforcement law. The jurisdictional requirement for recognition and enforcement of a foreign judgment is, in practice, closely related to the domestic jurisdictional requirements of U.S. courts. The jurisdictional basis of the EU court must therefore satisfy the "minimum contacts" requirement established in *International Shoe*.[139] Both uniform statutes in the United States also set out specific categories of jurisdiction that are deemed sufficient.[140] If the EU court that rendered the judgment is located where the judgment debtor has its establishment under Article 79(2), the judgment is likely to fall within the category where "the defendant had a business office in the foreign country and the proceeding in the foreign court involved a [cause of action] [claim for relief] arising out of business done by the defendant through that office in the foreign country."[141]

Where the judgment debtor has no EU establishment, however, the jurisdictional basis for enforcement under U.S. law is less certain. This may arise where jurisdiction under the GDPR is based on Article 3(2)'s targeting approach or on the data subject's habitual residence under Article 79. Both uniform statutes permit U.S. state courts, under section 5(b), to recognise jurisdictional bases other than the enumerated categories as sufficient to support a foreign-country judgment. Some courts have accepted additional bases of personal jurisdiction.[142] Still, the broader the EU jurisdictional basis, the more uncertain the prospects of enforcement in the United States.

The analysis above is based on U.S. law and may not apply generally to other jurisdictions. For example, enforcement of foreign judgments remains uncertain in China as a matter of practice, even though the latest amendments to the Civil Procedure Law offer a more certain set of rules and therefore a more positive outlook.[143] Ultimately, the effectiveness of private enforcement depends on the private international law of individual countries.

---

[136] In the common law tradition, the cause of action is merged into a judgment debt once a judgment is rendered. *See* Lord Collins of Mapesbury et al., *Dicey, Morris & Collins on the Conflict of Laws* (16th ed. 2022).

[137] *See supra* notes 128 and accompanying text.

[138] *See* King Fung Tsang & Tsz Wai Wong, Enforcement of Non-Monetary Judgments in Common Law Jurisdictions: Is the Time Ripe?, 45 Fordham International Law Journal 379 (2021); *see also* Sedona, *Enforceability of GDPR*, *supra* note 134, at 314.

[139] *Mercandino v. Devoe & Raynolds, Inc.*, 436 A.2d 1135 (N.J. Super. Ct. App. Div. 1981) ("In determining whether the Italian court had jurisdiction we deem it appropriate to apply the minimum contact test.").

[140] UFMJRA, § 5(a); UFCMJRA, *supra* note 135, § 5(a).

[141] UFCMJRA, § 5(a)(5); *see also* UFMJRA, *supra* note 135, § 5 (providing for a similar category). UFCMJRA, § 5(a) (enumerated categories); UFMJRA, § 5 (similar). Section 5(b) of each Act further permits recognition of non-enumerated jurisdictional bases. *See* Commissioners' Comment to UFCMJRA § 5(b) (2005).

[142] *See* Gary B. Born & Peter B. Rutledge, *International Civil Litigation in United States Courts* 1317 (8th ed. 2023).

[143] *See* Jie (Jeanne) Huang, *Recognition and Enforcement of Foreign Judgments in China After the 2023 Amendments to the Civil Procedure Law*, Neth. Int'l L. Rev. (2023).

There is, however, an important limitation. Because the cause of action does not arise from contract, the data subject cannot rely on party autonomy, i.e. forum selection, or arbitration clauses, to bind a foreign forum. GDPR private enforcement is instead channelled through the courts designated by the Regulation. In one U.S. case involving an alleged violation of the UK GDPR,[144] the court held that, because the UK GDPR expressly specifies that the action is to be brought in a UK court, it did not have "the power to enforce rights under the UK GDPR" and dismissed the case.[145] Since the EU GDPR contains a similar provision requiring data subjects to bring litigation in the courts of EU Member States,[146] Article 79 limits the judicial jurisdictional reach of GDPR private enforcement. Some U.S. courts have also declined to exercise jurisdiction because of lack of familiarity with the GDPR or because they considered the EU or UK to have stronger interests.[147]

This is where contractualized enforcement through submission clauses may be more effective. Depending on the drafting of the dispute resolution clauses, overseas litigation for breach of contract may be possible by the data exporter and, where applicable, by the data subject. As discussed above, EO 14117 gives parties freedom to decide on forum and governing law. Under the EU SCCs, contracting parties and data subjects may be able to sue in a foreign court under foreign law if the transfer contract falls within Module 4. Under the Chinese SCCs, contracting parties must apply Chinese law, but foreign arbitration may be possible.[148] Accordingly, private enforcement under the GDPR is not always as effective as a contractual claim under SCCs.

Even so, private enforcement remains superior to public enforcement in important respects. Public enforcement does not enjoy the same potential for foreign enforcement because of its public nature, a point recognised by the EU itself.[149] Private enforcement therefore makes USE statutes more effective overall.[150]

China largely follows the GDPR model. Under the PIPL, Article 50 expressly allows data subjects to bring litigation for violations of the PIPL. This right of private enforcement exists in addition to public enforcement and to any contractual rights under the Chinese SCCs.[151] Article 50 further provides that the private enforcement litigation must be brought in Chinese court.[152] This is understandable given that China does not have as many legal systems as EU does, and Hong Kong and Macau have their own data regulation regime that have not been harmonized with that of the Mainland.

The United States, by contrast, does not have a federal law with comparable extraterritorial reach regulating the USE of data. It would nevertheless be a mistake to conclude that the United States does not regulate data use or misuse extraterritorially. Instead, the United States does so through state statutes with extraterritorial effects and through traditional private law.

---

[144] *Cooper v. IBM*, 2023 U.S. Dist. LEXIS 83921.

[145] *Id.* at *12.

[146] GDPR art. 79.

[147] *See Doe v. Deutsche Lufthansa Aktiengesellschaft*, 2024 U.S. Dist. LEXIS 58281; *Elliott v. PubMatic, Inc.*; 2021 U.S. Dist. LEXIS 154053; *Finch v. Xandr, Inc.*, 2021 U.S. Dist. LEXIS 239963.

[148] *See supra* Feature 1.

[149] EDPB Report, *supra* note 123, at 28.

[150] *See* Lundstedt, *supra* note 132 (noting that, from a regulatory perspective, creation of private enforcement also lowers the monitoring costs of the government, as data subjects help police violations).

[151] Chinese SCCs art. 6(6).

[152] PIPL art. 50. This limitation is understandable given that, unlike the EU, China does not operate a network of harmonized legal systems: Hong Kong and Macau maintain their own distinct data regulation regimes that have not been aligned with mainland Chinese law.

As to state statutes, the extraterritoriality of California privacy legislation has been well publicised, and comparisons with the GDPR are common, despite its more limited scope, namely its focus on California residents.[153] For the purposes of this article, however, the more significant point is traditional case law. Data misuse may give rise to multiple claims in tort and contract. These ordinary private law claims may also have extraterritorial regulatory effects, although they are not usually described in those terms.[154] Compared with statutory private enforcement under the GDPR, such claims may have a higher chance of being entertained or enforced abroad, precisely because they appear as ordinary private law claims rather than as claims created by an expressly extraterritorial regulatory statute.

Tort law, in particular, is well known to have regulatory effects.[155] The *LICRA v. Yahoo!* litigation illustrates how tort or tort-like claims can regulate online conduct with cross-border effects.[156] In that case, Yahoo! was charged under tort law with hosting Nazi memorabilia auctions on its U.S. site, which was accessible in France.[157] The analogy is imperfect, since the case did not involve data privacy, but it shows how ordinary private law can be used to regulate cross-border internet activity.

That said, reliance on traditional private regulation comes with its own limitations. If the alleged misuse occurred abroad, it will often be difficult for a foreign court to apply U.S. law. Many jurisdictions give significant weight to the place of tort in their choice-of-law analysis, and U.S. choice-of-law rules also vary by state.[158] This is therefore the trade-off between creating a specific private enforcement right, such as the GDPR, and relying on traditional tort or contract claims. A specific statutory private right may more directly advance the regulatory scheme, but it may also be more visibly tied to extraterritorial public regulation. Traditional private rights claims may be more portable and less visibly extraterritorial, but their application is more heavily mediated by ordinary private international law rules.

C. Feature 3 – Private International Law Limitations for TAKE Regulation

Thus far, the features examined in this article have focused on GIVE and USE regulations on cross-border data. TAKE regulation, exemplified by the CLOUD Act in the United States and the E-Evidence Regulation in the European Union, is different. It is criminal or investigative in nature and therefore cannot rely on submission clauses or private enforcement in the same way as GIVE and USE regulations. It is also more intrusive. Unlike GIVE regulation, which regulates the outward transfer of data, and USE regulation, which regulates how data may be used, TAKE regulation compels an intermediary to produce data located abroad. As a result, legislating states have relied on self-imposed private international law limitations to mitigate the extraterritorial reach of such laws.

---

[153] *See, e.g.*, Anya E.R. Prince, *Comparing the GDPR and the California Consumer Privacy Act of 2018*, 93 S. Cal. L. Rev. 1 (2019), https://southerncalifornialawreview.com/wp-content/uploads/2020/01/93_1_Kessler.pdf.

[154] *See supra* Section II.A.

[155] *See, e.g.*, Symeon C. Symeonides, *The American Choice-of-Law Revolution: Past, Present and Future* (2006) (discussing the regulatory function of tort choice-of-law rules).

[156] LICRA v. Yahoo! Inc., T.G.I. Paris, May 22, 2000; *see also* Yahoo! Inc. v. La Ligue Contre Le Racisme et l'Antisémitisme, 433 F.3d 1199 (9th Cir. 2006) (en banc).

[157] *See* Jack L. Goldsmith & Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* 1–10 (2006).

[158] In California, although courts apply governmental interest analysis to tort claims, they will normally defer to the place of the tort as a presumption. *See McCann v Foster Wheeler LLC*, 48 Cal 4th 68, 97–98, 225 P3d 516, 534–35 (Cal 2010).

The Siberian Pipeline case suggests that the origin of data, by itself, cannot justify extraterritoriality.[159] Yet, this was precisely why export controls imposed before tangible goods or technological data left the territory might still be defended on territorial grounds: jurisdiction was exercised over tangible goods and technological data present within the United States, and the controls were imposed before those data left the United States, at a time when the United States clearly had jurisdiction under the territorial principle.[160] However, TAKE regulation is even more difficult to justify. It regulates source data while that data is abroad, and it does so merely by asserting control over intermediaries. Unlike GIVE and USE regulations, therefore, TAKE regulation has no direct territorial tie to the source data. This makes it more intrusive.

The prime example of a TAKE statute is the CLOUD Act under US law.[161] § 2713 gives the Department of Justice broad power to require intermediaries, by warrant, to turn over data in their possession, custody, or control, even if the data is located in a foreign country:

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, *regardless of whether such communication, record, or other information is located within or outside of the United States*.[162]

The immediate impetus for the CLOUD Act was the *Microsoft* case, in which the Department of Justice requested Microsoft to provide an email stored in Ireland under the Stored Communications Act (SCA).[163] Microsoft provided the customer's non-content information held in the United States to the government, but resisted producing the content of the email, which was the data in question and was located in its datacenter in Ireland.[164] The Second Circuit held that Congress had not intended the SCA's warrant provisions to apply extraterritorially. The focus of the provisions was the protection of the user's privacy interests, and the relevant application therefore concerned data stored abroad rather than conduct in the United States.[165] Accordingly, the Department of Justice was denied access to the email.[166] While the case was being appealed to the US Supreme Court, Congress quickly passed the

---

[159] EEC Comments, *in* A.V. Lowe, *Extraterritorial Jurisdiction* 201, 203 (1983) ("Goods and technology do not have any nationality and there are no known rules under international law for using goods or technology situated abroad as a basis of establishing jurisdiction over the persons controlling them.").

[160] Note, Extraterritorial Application of United States Law: The Case of Export Controls, 132 U. Pa. L. Rev. 355, 375–76 (1984) ("Jurisdiction is exercised over goods and technology present in the territory of the United States . . . . [Export controls] are imposed and made explicit before the goods leave the United States, at a time when the United States clearly has jurisdiction under the well established territorial principle. The imposition of those types of controls, therefore, is legitimate under international law.").

[161] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018) (codified as amended at 18 U.S.C. §§ 2523, 2713) [hereinafter CLOUD Act].

[162] 18 U.S.C. § 2713 (as amended by CLOUD Act, *supra* note 162). "Electronic communication service" and "remote computing service" are defined in 18 U.S.C. §§ 2510(15), 2711(2) (emphasis added).

[163] *Microsoft Corp. v. United States* (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) [hereinafter *Microsoft*].

[164] *Id.* at 200.

[165] *Id.* at 222.

[166] *Id*.

CLOUD Act to amend the SCA on a Department of Justice bill, so that the amended statute would have express extraterritorial effect.[167]

It is hard to justify the CLOUD Act by reference to traditional public international law grounds alone. In some cases, the requested data may relate to national security, such as a terrorism investigation,[168] and may therefore be linked to the passive personality principle.[169] But that will not always be so. The *Microsoft* case itself concerned narcotics trafficking.[170] The United States may argue that narcotics trafficking is sufficiently prejudicial to its national interest to justify extraterritoriality.[171] Yet the CLOUD Act does not set any threshold concerning the seriousness of the offence.[172] Moreover, both the passive personality principle and the protective principle remain controversial and have not been universally accepted.[173] The same applies to the effects doctrine, since data requested under the CLOUD Act may not always have a substantial effect in the United States.[174]

Instead of fitting the CLOUD Act neatly within a traditional public international law justification, the United States government has relied on multiple private international law mechanisms to soften its extraterritorial impact. The two most important are personal jurisdiction, or judicial jurisdiction, and the comity defence.

In the Department of Justice's Q&A, the Department emphasized that the CLOUD Act applies only to providers that are "subject to U.S. jurisdiction."[175] In explaining what US jurisdiction means, it stated that jurisdiction "is not limited to U.S. corporations, U.S. headquartered companies, or companies owned by U.S. persons. But neither is U.S. jurisdiction unlimited."[176] The Department's White Paper on the CLOUD Act similarly states that "[n]othing in the CLOUD Act changed the requirement that the United States must have personal jurisdiction over a company in order to require the disclosure of information the company holds."[177]

The question, then, is how an intermediary becomes subject to US personal jurisdiction. The answer appears to be the minimum contacts test developed by the US Supreme Court in *International Shoe*. The Department of Justice explains that "U.S. law limiting jurisdiction over foreign companies is based on constraints in the U.S. Constitution and has been developed by U.S. courts over many years."[178] In practice, this means either general or specific jurisdiction. For general jurisdiction, the Department states that "personal jurisdiction is most readily

---

[167] Cong. Rsch. Serv., R45173, *Cross-Border Data Sharing Under the CLOUD Act* 2, 7–8 (2018), https://www.congress.gov/crs_external_products/R/PDF/R45173/R45173.5.pdf. Stored Communications Act, 18 U.S.C. §§ 2701–2712, enacted as Title II of the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[168] *Microsoft*, 829 F.3d at 224.

[169] Crawford, *supra* note 15, at 445 (observing that there is almost "a consensus on the use of passive personality in certain cases, often linked to international terrorism").

[170] *Microsoft*, 829 F.3d at 200.

[171] *Id.* at 446.

[172] *Id.* (suggesting that the vital interest underlying the extraterritorial application still needs to be substantiated "beyond a vague sense of gravity").

[173] *See supra* note 126 (citing Mann).

[174] *See supra* note 122 (discussing the effects doctrine in relation to the GDPR).

[175] U.S. Dep't of Just., Frequently Asked Questions about the Clarifying Lawful Overseas Use of Data (CLOUD) Act, at 17 (Apr. 2019), https://www.justice.gov/criminal/media/999616/dl?inline.

[176] *Id.*

[177] U.S. Dep't of Just., *CLOUD Act White Paper* 17 (Apr. 10, 2019) ("U.S. jurisdiction is not limited to U.S. corporations, U.S. headquartered companies, or companies owned by U.S. persons. But neither is U.S. jurisdiction unlimited.").

[178] U.S. Dep't of Just., *supra* note 176, at 17.

established when a company is located in the United States."[179] This is consistent with the Supreme Court's modern formulation of general jurisdiction over corporations, under which the forum epitomises the "essential home" and "nerve centre" of a company,[180] with the paradigm cases being the place of incorporation and the principal place of business.[181] For specific jurisdiction, the Department states that whether "a foreign company located outside the United States but providing services in the United States has sufficient contacts with the United States to be subject to U.S. jurisdiction is a fact-specific inquiry turning on the nature, quantity, and quality of the company's contacts with the United States." It further explains that "the more a company has purposefully directed its conduct into the United States, the more likely a court will find the company is subject to U.S. jurisdiction."[182] A growing number of U.S. Supreme Court decisions also suggest the relevance of qualitative contacts to the particular dispute.[183]

It should be noted, however, that the CLOUD Act itself contains no express reference to the minimum contacts doctrine. Although the Department of Justice is correct to state that "U.S. law limiting jurisdiction over foreign companies is based on constraints in the U.S. Constitution and has been developed by U.S. courts over many years,"[184] the minimum contacts doctrine is generally a standard for judicial jurisdiction in civil litigation under private international law. Its application to criminal investigations is less certain. As one commentator has observed, while a foreign defendant in a tort, contract, or property action can challenge personal jurisdiction by invoking due process and minimum contacts doctrine, "when a foreign defendant is criminally prosecuted, there is, simply, nothing directly comparable."[185] Despite the uncertain relationship between minimum contacts and criminal investigations, the Department of Justice clearly treats the doctrine as an important mitigating factor in the CLOUD Act's extraterritorial reach.

The use of judicial jurisdiction as a limit on legislative jurisdiction is not new. As Justice Ginsburg stated in *RJR Nabisco, Inc. v. European Community*, extraterritorial application of RICO could be checked by doctrines that block litigation in US courts where cases are more appropriately brought elsewhere. Forum non conveniens allows courts to refuse jurisdiction where an alternative and more appropriate forum is available, and due process constraints on general personal jurisdiction protect foreign corporations from suit in the United States based on foreign conduct unless their affiliations with the forum are so constant and pervasive as to render them essentially at home there. These controls, Justice Ginsburg explained, "provide a check against civil RICO litigation with little or no connection to the United States."[186] This

---

[179] *Id.*

[180] *International Shoe 316–317; Ford Motor Co. v Mont*. Eighth Jud Dist. Ct. 141 S. Ct.1017, 1022 (2021); *Bristol-Myers Squibb Co. v. Superior Court of California, San Francisco County*, 582 U.S. 255. 260 (2017); *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 919 (2011).

[181] *Id*.

[182] *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) ("[D]ue process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'").

[183] US decisions on the significance of defendant's contacts in relation to a particular dispute/litigation: *Ford* at 1029, *Keeton* at 777; *McIntyre* at 891. *Bristol Myers* at 263.

[184] *Id.*

[185] Michael Farbiarz, *Accuracy and Adjudication: The Promise of Extraterritorial Due Process*, 116 Colum. L. Rev. 625 (2016) ("When a foreign defendant is sued in a tort action or on a contract or property claim, the defendant can challenge the court's power — its jurisdiction — by invoking a century's worth of due process jurisprudence . . . . But when a foreign defendant is criminally prosecuted, there is, simply, nothing directly comparable. With rare exceptions, the fundamental issue of the court's criminal power has not been considered by judges or by commentators or by litigators.").

[186] *RJR Nabisco, Inc. v. European Cmty*., 579 U.S. 325, 362 (2016).

stands in contrast to the jurisdictional formulation used in the Siberian Pipeline case, where US law expressly covered foreign subsidiaries under the control of US persons.[187] Given the substantial contraction of US general jurisdiction in recent years, personal jurisdiction can serve as a reasonable compromise in the extraterritorial application of the CLOUD Act.[188]

Yet it remains unclear whether the minimum contacts standard applies to intermediaries in the context of the CLOUD Act. The Supreme Court has never directly addressed whether nonparties have jurisdictional due process rights.[189] The applicability of minimum contacts to criminal cases is also unresolved. As observed by Smonwitz and Silberman, "[c]ourts have largely assumed that the jurisdictional analysis is the same for criminal grand jury subpoenas as it is for civil subpoenas, although this question remains open."[190] There is currently no case in which a court has applied the minimum contacts standard to a warrant issued to an intermediary under the CLOUD Act. Minimum contacts have, however, been applied in the context of an order issued under the All Writs Act in one Second Circuit case: "if jurisdiction over the subject matter of and the parties to litigation is properly acquired, the All Writs Act authorizes a federal court to protect that jurisdiction even though nonparties may be subject to the terms of the injunction."[191]

Even if minimum contacts are assumed to apply to the CLOUD Act, commentators have questioned whether Daimler's general jurisdiction framework should apply directly to nonparties who are not defendants in the underlying prosecution and therefore face different burdens.[192] A further complication comes from *Mallory*.[193] In that case, the Supreme Court held that a Virginia corporation was subject to jurisdiction in Pennsylvania because its registration under the Pennsylvania statute constituted consent. If a foreign intermediary has registered in the forum under a state statute, it may therefore be subject to the forum's general jurisdiction.[194]

After *Daimler*, some courts in civil subpoena cases have logically turned to specific jurisdiction, although the Supreme Court has not addressed specific jurisdiction over non-parties.[195] In *Gucci Am., Inc. v. Weixing Li*, the Second Circuit held that the district court had no general jurisdiction over Chinese banks asked to deliver information concerning Chinese defendants accused of selling counterfeit products. General jurisdiction could no longer rest on the banks'

---

[187] 47 Fed. Reg. 27,250 (1982) (June 22 Regulation applying export controls expressly to "any person subject to the jurisdiction of the United States," including foreign subsidiaries and licensees of U.S. technical data).

[188] *See Piper Aircraft Co. v. Reyno*, 454 U.S. 235 (1981) (forum non conveniens); Daimler AG v. Bauman, 571 U.S. 117, 139 (2014) (requiring corporation to be "essentially at home" in the forum for general jurisdiction); *Gulf Oil Corp. v. Gilbert*, 330 U.S. 501 (1947) (private and public interest factors for forum non conveniens). The contraction followed *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915 (2011), and *Daimler*, 571 U.S. 117 (2014), which replaced the earlier "doing business" test with the "essentially at home" standard. *See* Charles W. "Rocky" Rhodes, *The Predictability Principle in Personal Jurisdiction Doctrine: A Case Study on the Effects of Goodyear and Daimler*, 19 Lewis & Clark L. Rev. 733 (2015).

[189] Aaron D. Simowitz & Linda J. Silberman, *Jurisdiction over Nonparties Under the CLOUD Act*, 55 Vand. J. Transnat'l L. 425, 455 (2022), https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss2/5/ ("[T]he US Supreme Court has never explicitly held that nonparties to a suit have any jurisdictional due process right at all.").

[190] *Id.* at 454 n.104.

[191] *United States v. IBT*, 907 F.2d 277, 281 (2d Cir. 1990) ("[I]f jurisdiction over the subject matter of and the parties to litigation is properly acquired, the All Writs Act authorizes a federal court to protect that jurisdiction even though nonparties may be subject to the terms of the injunction.").

[192] Simowitz & Silberman, *supra* note 190, at 434–35.

[193] *Mallory v. Norfolk S. Ry. Co*., 600 U.S. 122 (2023). *Cf. Bauxites de Guinée, S.A. v. Alcoa, Inc*., 456 U.S. 694 (1982) (consent to jurisdiction through prior conduct).

[194] *See also* Simowitz & Silberman, *supra* note 190, at 453 .

[195] *Gucci Am., Inc. v. Weixing Li*, 768 F.3d 122, 136 (2d Cir. 2014).

"doing business" in the forum after *Daimler*.[196] On remand,[197] specific jurisdiction was found because "BOC frequently and deliberately used its New York correspondent account with Chase to effectuate wire transfers for its U.S. clients, including, critically, Defendants in this action."[198] The court, however, did not make clear whether the relevant nexus was with the underlying claim or with the discovery order itself.[199] If the former is required, specific jurisdiction would be much harder to establish.[200] If the latter is sufficient, specific jurisdiction would be easier to establish where the evidence in question was generated by conduct in the forum.[201] Applying this logic to the CLOUD Act, if the email in *Microsoft* was first processed in the United States and only subsequently stored overseas, specific jurisdiction would likely be easier to establish.[202]

Overall, despite uncertainty over the application of minimum contacts to nonparties in the CLOUD Act context, personal jurisdiction appears to be a significant limitation on the Act's extraterritorial effect. This is a substantial difference from the US jurisdiction basis in the Pipeline case.[203] The CLOUD Act's reliance on personal jurisdiction therefore represents a meaningful improvement in reducing the risk of backlash from the international community.

The practical effect of this limitation is important. For general jurisdiction, only companies incorporated in the United States or having their principal place of business in the United States will ordinarily be treated as "at home" in the United States, subject to the complication introduced by consent-based jurisdiction after *Mallory*. On this understanding, it may be difficult for the Department of Justice to obtain evidence located abroad from a foreign subsidiary merely because its parent company has US contacts. *Daimler* held that the contacts of a California subsidiary could not render the German parent subject to general jurisdiction in California, even though the subsidiary contributed roughly ten percent of the parent's worldwide revenue. The reverse should also be true: the contacts of a domestic parent should not automatically be attributed to a foreign subsidiary. Thus, US courts would not necessarily have general jurisdiction over Microsoft's Irish subsidiary in the original *Microsoft* litigation.[204]

It is true that the warrant could be directed at Microsoft in the United States and require it to procure the data from its Irish subsidiary. But that is precisely the kind of move that resembles the Pipeline scenario and triggers foreign protest. It would also undermine the mitigating purpose of using personal jurisdiction as a limiting standard in the first place.

The better answer probably lies in specific jurisdiction. Although the application of specific jurisdiction in the criminal context of the CLOUD Act remains uncertain, an analogy may be drawn from trademark infringement cases in which Chinese banks were required to provide evidence. In *Gucci* and *Nike v. Wu*, Chinese banks were held to be subject to New York's specific jurisdiction because they used the New York banking system to facilitate transactions

---

[196] *Id.* at 135.

[197] *Id.* at 145.

[198] *Gucci Am., Inc. v. Weixing Li*, 135 F. Supp. 3d 87, 95 (S.D.N.Y. 2015).

[199] Simowitz & Silberman, *supra* note 190, at 449.

[200] *Id.* at 436 ("If the nexus had to be with the underlying action, discovery could only be had from a nonparty if it had contacts in the US forum connected with the plenary action against the defendant, a difficult standard to satisfy.").

[201] *Id.* at 474.

[202] The processing location is not made entirely clear in the case. *See Microsoft*, 829 F.3d at 203.

[203] *See supra* note 193.

[204] *Daimler*, 571 U.S. at 136 n.13, 139 n.20 (rejecting attribution of subsidiary's California contacts to the German parent for general jurisdiction purposes). *Cf.* Bard v. Daimler AG, No. 22-1591 (1st Cir. 2023) (declining to attribute U.S. subsidiary contacts to the German parent). The precise scope of reverse attribution remains unsettled across the circuits.

connected with the alleged counterfeiting activities.[205] If this standard applies in the CLOUD Act context, many foreign intermediaries may be subject to US specific jurisdiction where the relevant data traffic passes through the United States or makes use of US infrastructure. The key difference between this approach and compelling a US parent to produce data held by a foreign subsidiary lies in the nature of the connection. In the specific jurisdiction model, the United States seeks data that has a connection with the investigation, the relevant service, or the infrastructure used in the United States. Whether that connection is sufficient and reasonable will remain contestable in individual cases. But it is a superior theory to the much-condemned treatment of foreign subsidiaries as US nationals in the Pipeline case. Indeed, F.A. Mann argued that traditional jurisdictional justifications should be replaced by an analysis of connection, an idea originally derived from private international law.[206]

Another safeguard under the CLOUD Act is the comity defence, under which an intermediary may resist a warrant where it reasonably believes: "(i) that the customer or subscriber is not a United States person and does not reside in the United States; and (ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government."[207] If both conditions are satisfied, the court must determine, "based on the totality of the circumstances," whether "the interests of justice dictate" that the legal process should be modified or quashed.[208] The statute requires the court to consider multiple factors, including the interests of the United States, the interests of the qualifying foreign government in preventing any prohibited disclosure, the penalties to the provider, the location and nationality of the data subject, the nature and extent of the provider's ties to and presence in the United States, the importance to the investigation of the information, the availability of alternative access to the information, and the investigative interests of the foreign authority making the request for assistance.[209]

This defence is significant because it addresses what has long been recognized as the primary burden on foreign nonparties: the "vice of foreign compulsion," where foreign law prohibits what US law requires.[210] This defence will be triggered when there is a conflict between the CLOUD Act and foreign law, and the US has not entered into an executive agreement with the foreign country in question for reciprocal enforcement.[211]

This comity defence can be traced to choice-of-law analysis under the Restatement Second of Conflict of Laws.[212] Lowenfeld's proposed criteria for assessing extraterritorial regulation included the character of the regulated activity, the policies underlying the regulation, the link between the regulating state and the persons whose activity is regulated, the needs and traditions of the international system, justified expectations, the certainty and intensity of conflict, the territory where the regulated activity is principally carried on, the direct and

---

[205] *See Gucci Am., Inc. v. Weixing Li*, 768 F.3d 122 (2d Cir. 2014); *Tiffany (NJ) LLC v. Qi Andrew*, 276 F.R.D. 143 (S.D.N.Y. 2011).

[206] *Nike, Inc. v. Wu*, 349 F. Supp. 3d 346, 361 (S.D.N.Y. 2018); *see also Gucci Am., Inc. v. Weixing Li*, 135 F. Supp. 3d 87, 95 (S.D.N.Y. 2015) (specific jurisdiction based on use of New York correspondent banking accounts).

[207] CLOUD Act, *supra* note 162, § 2713(2)(A) (codified at 18 U.S.C. § 2713(2)(A)).

[208] 18 U.S.C. § 2713(2)(B).

[209] 18 U.S.C. § 2703(h)(3).

[210] To date, the United Kingdom and Australia have entered into such arrangements with the United States. For an alternative understanding of the "comity" concept, *see* Peari, 2018, at 151-155.

[211] The term "foreign compulsion" is used in Restatement (Third) of Foreign Relations Law § 441 (Am. L. Inst. 1987) (setting out foreign-state compulsion as a defense to violation of U.S. law); *see also* A.V. Lowe, *Extraterritorial Jurisdiction* 110 (1983).

[212] Restatement (Second) of Conflict of Laws § 6 (Am. L. Inst. 1971).

foreseeable effects of the conduct, and the legislature's specific intention to regulate the conduct at issue.[213]

A similar concept can be traced even earlier to F.A. Mann's 1964 Hague lecture. Mann argued that extraterritoriality should not be approached through fixed traditional heads of jurisdiction, but through a search for the state or states whose contacts with the facts make the allocation of legislative competence just and reasonable: "The problem, properly defined, involves the search for the State or States whose contacts with the facts is such as to make the allocation of legislative competence just and reasonable. It is, accordingly, not the character and scope inherent in national legislation or attributed to it by its authors, but it is the legally relevant contact between such legislation and the given set of international facts that decides upon the existence of jurisdiction."[214] Like Lowenfeld, Mann expressly drew inspiration from choice of law in private international law: "As soon as attention is directed to the connection of facts with certain States, it becomes the foremost task, for purposes of international jurisdiction no less than for purposes of the choice of law in private international law, to identify the relevant points of contact, to localise the legal relationships."[215] Sixty years later, Mann's connection-based approach remains widely recognized in contemporary thinking about extraterritoriality: "If there is a cardinal principle emerging, it is that of genuine connection between the subject matter of jurisdiction and the territorial base or reasonable interests of the state in question."[216]

It must be noted that this choice-of-law-inspired, case-by-case comity approach is no longer the prevailing approach to extraterritoriality in the United States.[217] The adoption of this approach by the US government in the CLOUD Act, together with the minimum contacts limitation, therefore suggests the intentional use of private international law techniques to soften this particularly intrusive TAKE statute. Since TAKE regulation cannot be implemented through contract and does not lend itself to private enforcement, judicial jurisdiction and comity serve as the most available private international law techniques. These techniques also appear in the latest EU E-Evidence Regulation, which will soon come into force.

Less than a month after the CLOUD Act was enacted, the European Union proposed a similar TAKE regulation.[218] The EU eventually enacted the E-Evidence Regulation in 2023.[219] The

---

[213] Andreas F. Lowenfeld, *Public Law in the International Arena: Conflict of Laws, International Law, and Some Suggestions for Their Interaction*, 74 Am. Soc'y Int'l L. Proc. 30, 31–32 (1980) (proposing nine criteria, in part borrowed from the Restatement of Conflict of Laws, for assessing the reasonableness of extraterritorial regulation). This approach was subsequently adopted by Restatement (Third) of Foreign Relations Law § 403(1) (Am. L. Inst. 1987), which also expressly recognized the influence of choice of law from the Restatement Second of Conflict of Laws. *See id.* § 403 reporters' note 10 ("The factors set forth in the present section . . . adopt the factors listed in § 6 of the Restatement, Second, of Conflict of Laws, and take account of developments in the practice of other states.").

[214] Mann, *The Doctrine of Jurisdiction*, *supra* note 12, § VI.

[215] *Id.*

[216] Mann, *The Doctrine of Jurisdiction*, *supra* note 12, at § VI; *see also* Ian Brownlie, *Principles of Public International Law* 441 (8th ed. 2012); *see also* Jennifer Daskal, *Investigative Jurisdiction: The Evolving Limits of Extraterritoriality in Transnational Digital Investigations*, 73 Int'l & Comp. L.Q. 271, 280 (2024) [hereinafter Daskal, *Investigative Jurisdiction*] (referring, among others, to Mann's theory).

[217] Hannah L. Buxbaum, *Extraterritoriality in the Public and Private Enforcement of U.S. Regulatory Law*, 236, 250 (Diego P. Fernández Arroyo & Franco Ferrari eds., 2019) ("In private enforcement, by contrast, there seems to be a significant shift away from the consideration of foreign interests as part of jurisdictional analysis. The high water mark for a multilateral-style analysis in private regulatory claims dates to the Restatement (Third) era.").

[218] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM (2018) 225 final (Apr. 17, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN. The CLOUD Act was enacted on March 23, 2018.

[219] Regulation (EU) 2023/1543, of the European Parliament and of the Council of 12 July 2023, on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings, 2023 O.J. (L 191) 118 [hereinafter E-Evidence Regulation].

Regulation permits an authority of a Member State, in criminal proceedings, to order a service provider "offering services in the Union" to produce or preserve electronic evidence.[220] It applies to service providers without an establishment in the EU, and its application does not depend on the location of the data.[221] Like the CLOUD Act, therefore, it has clear extraterritorial reach.[222]

Commentators have noted the similarities between the E-Evidence Regulation and the CLOUD Act, especially the shift away from data location as the key determinant of jurisdiction.[223] It is therefore unsurprising that the E-Evidence Regulation also uses the same two private international law techniques as the CLOUD Act to mitigate its extraterritorial reach.

Like the CLOUD Act, the E-Evidence Regulation limits its application by reference to service providers subject to its jurisdiction.[224] Article 3 defines "offering services in the Union" broadly as: "(a) enabling natural or legal persons in a Member State to use the services; and (b) having a substantial connection." "Substantial connection" is in turn defined as including (i) where the service provider has an establishment in a Member State, or (ii) where there are a significant number of users in one or more Member States, or (iii) where there is targeting of activities towards one or more Member States.[225]

Intermediaries are therefore intentionally not limited to those with an EU establishment, defined as "an entity that actually pursues an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or the business is managed."[226] The reason is that the EU recognizes that "in many cases, data are no longer stored or otherwise processed on a user's device but made available on a cloud-based infrastructure enabling access from anywhere."[227] Thus, where there is no EU establishment, a substantial connection may still be found where there is a significant number of EU users or where the provider targets activities toward the EU.[228]

The targeting analysis is determined by all relevant circumstances, including: (i) the use of a language or currency generally used in the Member State; (ii) the possibility of ordering goods or services; (iii) the availability of an application in the relevant national app store; (iv) the provision of local advertising or advertising in the language generally used in the Member State; (v) the handling of customer relations; and (vi) whether the provider directs its activities toward one or more Member States as understood in the Brussels I Regulation.[229] The final reference is particularly important. Unlike the CLOUD Act, which refers directly to judicial jurisdiction

---

[220] E-Evidence Regulation art. 1.

[221] *Id.*

[222] COM (2018) 225 final, *supra* note 219. The timing is significant: the EU proposal came only 25 days after the CLOUD Act was signed into law on March 23, 2018, suggesting the Commission had been closely monitoring U.S. legislative developments. *Cf.* Jennifer Daskal, The Opening Salvo: The CLOUD Act, E-Evidence Proposals, and EU–US Discussions Regarding Law Enforcement Access to Data Across Borders, in The Cambridge Handbook of Cyber Behavior 329 (2024) [hereinafter Daskal, Opening Salvo] (analysing the relationship between the two instruments).

[223] *See* Daskal, *Opening Salvo*, *supra* note 223.

[224] Daskal, *Investigative Jurisdiction*, *supra* note 216, at 700.

[225] E-Evidence Regulation art. 3(2)(a)–(b). Covered services include electronic communications services and internet domain name and IP numbering services. *See id.* art. 3(1).

[226] E-Evidence Regulation art. 3(5).

[227] E-Evidence Regulation recital 21.

[228] E-Evidence Regulation art. 3(5). This definition of "establishment" tracks the concept developed in EU freedom-of-services case law. *See* Case C-221/89, *R. v. Secretary of State for Transport, ex parte Factortame Ltd.*, ECLI:EU:C:1991:320 (establishing the stable infrastructure test).

[229] E-Evidence Regulation recital 30.

under the US Constitution, the EU does not simply delegate the matter to the general judicial jurisdiction rules under the Brussels I Regulation. Instead, it incorporates part of that approach while supplementing it with specific factors designed for electronic evidence. Nevertheless, the similar use of judicial jurisdiction as a limitation on extraterritoriality is evident. It may also be argued that the dual prongs of establishment and targeting resemble the general and specific jurisdiction categories in minimum contacts doctrine. The establishment prong appears broader than US general jurisdiction, which primarily covers place of incorporation and principal place of business,[230] but both turn on a stable and concrete presence in the forum. The multi-factor targeting prong resembles the purposeful availment approach in US specific jurisdiction and departs from the more rule-based approach to special jurisdiction under the Brussels I Regulation.[231]

The E-Evidence Regulation also incorporates a comity defence. Recital 74 expressly recognizes the concern that compliance with a European Production Order may conflict with the law of another country. The Regulation therefore provides a specific mechanism for judicial review of that conflict in Chapter IV. Where the competent court establishes that the foreign law prohibits disclosure of the data concerned, it must determine whether to uphold or lift the European Production Order based on the consideration of a number of factors.[232] These factors include the strength of the third country's interest in preventing disclosure, including any fundamental rights or national security concerns at stake; how closely the underlying criminal case connects to each jurisdiction, judged by the location, nationality, and residence of the data subject or victim and by where the offence was committed; how closely the service provider itself is connected to the third country; the investigating state's interest in obtaining the evidence, given the offence's seriousness and the need for timely access; and the consequences, including potential penalties, that compliance would carry for the addressee or provider.

These factors are plainly similar to those under the CLOUD Act's comity defence, although there are differences.[233] Recital 78 specifically emphasizes that, in weighing these factors, "particular importance and weight should be given to the protection of fundamental rights by the relevant law of the third country."[234] It has been noted that this comity defence is the first of its kind in EU legislation in the criminal justice context.[235] As discussed above in relation to the CLOUD Act, this kind of comity defence is heavily influenced by choice-of-law reasoning in the United States. Thus, even though interest analysis is not generally adopted as a choice-of-law technique in the EU, the private international law influence is undeniable.[236]

Commenting on these mitigating mechanisms, Ryngaert observes that "[s]trikingly, these principles also draw on the law of prescriptive jurisdiction, in particular the notions of genuine connection and reasonableness."[237] In summary, because TAKE regulation is especially intrusive, it requires stronger limiting principles. Those principles are found in private

---

[230] *Mallory* has extended general jurisdiction to some extent. *See supra* note 193 and accompanying text.

[231] E-Evidence Regulation recital 30. The sixth factor expressly cross-references the purposeful direction test from *Pammer v. Reederei Karl Schlüter GmbH & Co. KG* (C-585/08) and *Hotel Alpenhof GmbH v. Heller* (C-144/09), ECLI:EU:C:2010:740, tying the E-Evidence targeting standard to established EU private international law doctrine.

[232] E-Evidence Regulation art. 17(6).

[233] *See* Daskal, *Investigative Jurisdiction*, *supra* note 217, at 698.

[234] E-Evidence Regulation recital 78.

[235] Daskal, *Investigative Jurisdiction*, *supra* note 217, at 697.

[236] *Id.* (noting the novelty and arguing that the E-Evidence comity defence represents a significant convergence between EU criminal justice law and U.S.-style interest balancing).

[237] Cedric Ryngaert, *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*, 24 German L.J. 537, 546 (2023).

international law. Theoretically, the justification for extraterritoriality depends on a sliding scale of connections. Rules on judicial jurisdiction and comity defence provide the connection-based limits that make the extraterritorial application of TAKE regulation more defensible. Whether the current standards of connection are sufficient in any individual case remains open to debate. But that is the foundational idea behind the rule.

D. Feature 4 – Private International Law as Defense to Extraterritoriality

Beyond the three types of extraterritorial data regulations (GIVE, USE and TAKE), one may further argue that there is a fourth type: DEFENSE regulations. For the most part, these consist of blocking statutes. While there is no universally accepted definition, blocking statutes generally refer to domestic laws designed to restrict and counter the extraterritorial effect of foreign laws or measures with extraterritorial impact.[238] Although blocking statutes are usually not data-specific, recent Chinese legislation has expressly included data and personal information within the scope of defensive countermeasures against foreign extraterritorial regulation.[239]

DEFENSE regulations are themselves deeply intertwined with private international law and naturally make broad use of private international law mechanisms in resisting the extraterritorial effect of foreign statutes. This development is unsurprising given the extensive use of private international law techniques in the GIVE, USE and TAKE regulations discussed above.

In addition to DEFENSE statutes, there are other defensive strategies making use of private international law, including conflict avoidance through data centralisation and reciprocal arrangements.

1. Blocking Statutes

The first modern blocking statute was the UK Protection of Trading Interests Act discussed in Section III. If anything, the Pipeline case demonstrates the effectiveness of blocking statutes in containing extraterritorial regulation. It is therefore unsurprising that many jurisdictions have since adopted similar legislation, including the EU and China,[240] and such statutes may potentially be deployed against extraterritorial data regulation as well.[241]

As discussed in Section III,[242] the UK Protection of Trading Interests Act sought to counter extraterritorial regulation in three principal ways: non-compliance, denial of judgment enforcement, and claw-back provision

---

[238] Adrian Hemler, *Deconstructing Blocking Statutes: Why Extraterritorial Legislation Cannot Violate the Sovereignty of Other States*, 21 J. Priv. Int'l L. 115, 115-116 (2025). [hereinafter Blocking Statute Article]; *see also* Born & Rutledge, *supra* note 143.

[239] *See* Ministry of Ecology and Environment Regulation, art. 9, [hereinafter MEE Regulation]; *see also* Regulations on the Implementation of the Anti-Foreign Sanctions Law of the People's Republic of China, arts. 8(4), 17 [hereinafter AFSL Regulations] (expressly authorising prohibition or restriction of data and personal information transfers as countermeasures against foreign extraterritorial measures).

[240] Blocking Statute Article, at 117 (listing France, Mexico, and Canada among jurisdictions adopting similar measures).

[241] *See* MEE Regulation art. 9 (referring specifically to data and personal information). Lowe, *Blocking Extraterritorial Jurisdiction*, *supra* note 46, at 257. Some commentators trace earlier precursors to the Danish statute of 1967, enacted in response to U.S. shipping antitrust investigations. *See* Blocking Statutes Article, *supra* note 239, at 116.

[242] *See supra* Section III.

Both the EU and Chinese blocking regimes broadly follow this blueprint and provide mechanisms corresponding to all three forms of countermeasures.[243] In substance, the three mechanisms correspond closely with the three major branches of private international law.

The non-compliance mechanism effectively denies recognition, and thus the potential application, of foreign law through domestic choice of law rules.[244] Some commentators further characterize blocking statutes as overriding mandatory rules.[245] Importantly, non-compliance obligations are not absolute. Both EU and Chinese regimes provide mechanisms under which compliance may be permitted where non-compliance would cause serious hardship or disproportionate damage.[246]

At least under the EU framework, this gives rise to a balancing exercise resembling a multi-factor choice of law analysis. Article 3 of Implementing Regulation (EU) 2018/1101 requires applicants to demonstrate that non-compliance would cause "serious damage" to protected interests.[247] In *Bank Melli Iran v. Telekom Deutschland GmbH*,[248] the ECJ further held that proportionality requires balancing the objectives underlying the blocking regulation against the probability and extent of economic loss likely to be suffered by the affected party.[249] This balancing exercise is similar to the comity and conflict analysis discussed above in relation to the CLOUD Act discussed above. Such overlap is unsurprising. Multinational corporations frequently find themselves caught between competing legal obligations, namely compliance with the extraterritorial foreign measure on the one hand and compliance with the blocking statute on the other.

The denial of judgment enforcement mechanism similarly reflects established private international law principles. It effectively codifies the traditional rule against the recognition and enforcement of foreign public law judgments.[250]

Finally, the claw-back mechanism operates through judicial jurisdiction rules. Under the EU Blocking Statute, private recovery actions may be brought against any person, including intermediaries, subject to the jurisdiction of Member State courts pursuant to the Brussels Convention.[251] The Chinese blocking statutes are less specific and merely provide that such claims may be pursued before Chinese courts without clarifying whether jurisdiction exists automatically whenever the blocking statute applies or remains subject to ordinary judicial

---

[243] The Chinese blocking framework comprises multiple statutes and regulations. *See e.g.*, AFSL Regulations; Ministry of Commerce, *Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures* (Jan. 9, 2021) [hereinafter MOFCOM Rules]; MEE Regulation; Anti-Foreign Sanctions Law of the People's Republic of China (2021); National Security Law of the People's Republic of China (2015); Law on Foreign Relations of the People's Republic of China (2023). For the three principal measures, see MOFCOM Rules art. 7(1) (non-compliance order); art. 9 (claw-back); AFSL Regulations arts. 18–19 (non-compliance and non-enforcement of foreign judgments). *See also* Council Regulation 2271/96, of 22 November 1996, Protecting Against the Effects of the Extra-territorial Application of Legislation Adopted by a Third Country, arts. 4–6, 1996 O.J. (L 309) 1 [hereinafter EU Blocking Statute]; for EU Blocking Statute, *see* art 5 for non-compliance; art 4 for non-enforcement; and art 6 for clawback.

[244] Blocking Statute Article, at 132.

[245] *Id.* at 132–33.

[246] EU Blocking Statute art. 5(2); *see also* MOFCOM Rules art. 7(2) ("The prohibition order may be suspended or withdrawn by decision of the working mechanism based on actual circumstances.").

[247] Commission Implementing Regulation (EU) 2018/1101, of 3 August 2018, laying down the criteria for the application of the second paragraph of Article 5 of Council Regulation (EC) No 2271/96, 2018 O.J. (L 199 I) 7.

[248] Case C-124/20, *Bank Melli Iran v. Telekom Deutschland GmbH*, ECLI:EU:C:2021:1035 (Dec. 21, 2021).

[249] *Id*.

[250] *See* Lowe, *supra* note 35; *see also* Blocking Statute Article, *supra* note 239, at 132.

[251] EU Blocking Statute art. 6.

jurisdiction rules.[252] Regardless of the precise jurisdictional structure, claw-back provisions necessarily depend upon domestic courts for implementation and judicial jurisdiction therefore performs an important enabling function.[253]

It could be further argued that blocking statutes are not merely utilizing features of private international law, but themselves form part of private international law. As discussed in Section II, FA Mann distinguished between the role of public international law in setting the outer limits of jurisdiction and the role of domestic private international law in implementing jurisdictional claims in practice.[254] Given the absence of centralized enforcement mechanisms in public international law,[255] it is perhaps inevitable that when extraterritorial regulation exceeds the limits imposed by public international law, domestic private international law mechanisms assume the role of policing such excesses through blocking statutes.

The effectiveness of these private international law countermeasures varies depending upon the type of extraterritorial data regulation and the extent to which private international law techniques are embedded within the relevant regulatory framework.

For GIVE regulation, blocking statutes are likely to be comparatively less effective because they extensively utilizes submission clauses. In order for blocking statutes to apply in the first place, most regimes require, either expressly or implicitly, some form of violation of international law or the basic principles of international relations as well as harm to national interests. [256] As argued above under Feature 1, however, submission clauses arguably place GIVE regulation on stronger footing under public international law by relying upon consent.

Accordingly, the submission-clause dimension of GIVE regulation may not trigger blocking statutes in the first place. Even where blocking statutes are engaged, each of the corresponding private international law countermeasures applies less naturally. For non-compliance, the relevant provisions generally target foreign public law measures rather than private contractual obligations. For denial of enforcement, it may further be argued that a judgment based upon breach of contract, rather than a direct cause of action created by the foreign statute itself, falls outside the ordinary scope of blocking mechanisms.

USE regulation, which incorporate fewer private international law techniques, are comparatively more vulnerable to blocking statutes. It is more difficult to characterize USE regulation as purely private ordering even where private enforcement mechanisms exist. Accordingly, although similar arguments may be advanced in relation to SCC-based obligations, it becomes more difficult to resist denial of enforcement where the cause of action derives directly from the statute itself rather than breach of contract.

Finally, TAKE regulation, representing the most aggressive form of extraterritorial data regulation and incorporating the fewest private international law features, are likely to be the most susceptible to blocking statutes. All three countermeasures therefore become potentially applicable. Indeed, the CLOUD Act has already prompted recalibration of blocking legislation in jurisdictions such as France. TAKE statutes may further trigger additional forms of

---

[252] MOFCOM Rules art. 9.

[253] Chinese blocking statutes provide additional mechanisms such as a blacklist of entities, although such mechanisms are not in themselves private international law measures.

[254] *See supra* notes 24-26 and accompanying text.

[255] Blocking Statute Article, *supra* note 239, at 133 ("[I]nternational law cannot be effectively enforced on the international plane.").

[256] *See* MOFCOM Rules art. 2; art. 6(1) (listing "whether international law or the basic principles of international relations are violated" as a factor); *see also* AFSL Regulationsart. 6(1); EU Blocking Statute; MOFCOM Rules art. 6 (criteria including harm to national interests).

DEFENSE regulation beyond blocking statutes themselves, particularly GIVE-style restrictions. For example, compliance with the CLOUD Act may *prima facie* violate Article 48 of the GDPR.[257]

Nevertheless, even in the context of TAKE regulation, private international law mechanisms remain capable of mitigating extraterritorial conflict through comity-based defences and balancing techniques, thereby reducing the likelihood of triggering blocking statutes in the first place. Private international law therefore remains relevant in the TAKE context, albeit functioning more indirectly than in GIVE or USE regulation.

Finally, blocking statutes themselves are often carefully designed not to operate extraterritorially. For example, the UK Protection of Trading Interests Act expressly excludes two categories of persons from utilizing the claw-back mechanism: (i) companies incorporated in the foreign state issuing the extraterritorial regulation; and (ii) activities occurring exclusively within that foreign state in subsections 6(2) and (3).[258] As Lowe observed, "[t]he clawback system is primarily intended to neutralize foreign claims to excessive jurisdiction over British businesses. The exceptions in subsections 6(2) and (3), under which 'qualifying defendants' are denied the right to recover where they had strong links with the foreign state concerned, confine the scope of the section substantially. In essence, the right exists only against 'extraterritorial' judgments of the foreign court."[259]

Similarly, the EU Blocking Statute cannot ordinarily be invoked by subsidiaries of EU companies incorporated in the United States. According to the Commission Guidance Note, subsidiaries incorporated under US law are treated as US rather than EU operators and therefore fall outside the scope of the Blocking Statute,[260] although the position under Chinese blocking legislation remains less clear.[261]

2. Data Centralisation

Beyond DEFENSE regulation, some states also engage in data centralisation.[262] As discussed above, blocking statutes frequently generate conflict of laws problems by forcing intermediaries to choose between competing legal obligations.[263] Data centralisation, however, may reduce such conflicts through a form of "conflict avoidance." The term was originally

---

[257] GDPR art. 48; EDPB Report, *supra* note 123, at 22–23 (discussing the CLOUD Act–GDPR conflict). European Data Protection Board & European Data Protection Supervisor, *Joint Response to the LIBE Committee on the Impact of the US Cloud Act on the European Legal Framework for Personal Data Protection*, at 4 (July 10, 2019)(taking the view that "currently, unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, the lawfulness of such transfers of personal data cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject").

[258] Protection of Trading Interests Act 1980, c. 11, § 6(2)–(3) (UK).

[259] Lowe, *Blocking Extraterritorial Jurisdiction*, *supra* note 46, at 280 ("The clawback system is primarily intended to neutralize foreign claims to excessive jurisdiction over British businesses . . . . In essence, the right exists only against 'extraterritorial' judgments of the foreign court.").

[260] *See* Commission Guidance Note, *Questions and Answers: Adoption of Update of the Blocking Statute*, Q. 21, 2018 O.J. (C 277 I) 4.

[261] *See supra* note 244 and accompanying text. Unlike the EU Blocking Regulation, the MOFCOM Rules and the AFSL Regulations contain no express provision excluding subsidiaries incorporated in the foreign state. Whether a Chinese company's U.S. subsidiary falls within the scope of Chinese blocking measures therefore remains an open question of statutory interpretation.

[262] Russia also imposes data localisation requirements. *See* Federal Law No. 242-FZ (Russ.) (2014).

[263] *See supra* Feature 1 (discussing conflict avoidance through governing law clauses).

used to describe the avoidance of conflict of laws through *ex ante* governing law clauses.[264] Data centralisation arguably achieves a similar objective through territorial control over the location of data.[265]

China provides the clearest example. Under its GIVE regime, China permits certain cross-border transfers through SCCs.[266] At the same time, critical information infrastructure operators are generally required to store relevant data within China.[267] Companies processing data above specified thresholds are similarly prevented from relying solely on SCCs and instead require governmental approval before transferring data abroad.[268]

Although data centralisation does not eliminate conflict entirely, it may substantially reduce overlapping regulatory exposure. The *Microsoft* litigation illustrates the point. Suppose Tencent, a Chinese intermediary, stores an email exchanged between a US user and an Irish user on servers located in Ireland. If the DOJ subsequently requests disclosure of the email under the CLOUD Act, Tencent may simultaneously become subject to US, EU and Chinese law. The CLOUD Act may apply extraterritorially once minimum contacts with the United States are established, which would likely be satisfied where Tencent's email service is used by a US person. Since the data is stored in Ireland where Tencent has an establishment, the GDPR potentially applies. Tencent, as a Chinese company, also remains subject to Chinese law.[269]

Requiring the data to be stored in China from the outset reduces this three-way conflict into a two-way conflict. More importantly from China's perspective, territorial control over the location of the data provides China with ultimate control over whether the data may be transferred abroad, even where Tencent itself may still face penalties for non-compliance with US law. France has considered similar localization-oriented measures in response to the CLOUD Act.[270]

Data centralisation, however, is not without commercial cost. Localization requirements may discourage intermediaries from operating within the jurisdiction. As demonstrated by the *Microsoft* case, storing data geographically closer to users also produces technical and

---

[264] Georges R. Delaume, *The European Convention on the Law Applicable to Contractual Obligations: Why a Convention?*, 22 Va. J. Int'l L. 105, 115 (1981).

[265] The term "conflict avoidance" was coined in the governing-law-clause context by Delaume, *supra* note 265. Data centralisation achieves an analogous result through territorial control of data location rather than ex ante contractual choice of law.

[266] *See supra* notes 84–91 and accompanying text.

[267] *See supra* note 87 and accompanying text.

[268] Measures for the Standard Contract for the Cross-Border Transfer of Personal Information, art. 4 (Cyberspace Admin. of China, Feb. 24, 2023) (providing that a personal information handler may use the SCC route only if it (i) is not a critical information infrastructure operator; (ii) processes the personal information of fewer than 1,000,000 individuals; (iii) has cumulatively transferred the personal information of fewer than 100,000 individuals abroad since January 1 of the previous year; and (iv) has cumulatively transferred the sensitive personal information of fewer than 10,000 individuals abroad since January 1 of the previous year).

[269] This hypothetical is illustrative. The choice of Tencent and Ireland is deliberate: Tencent operates substantial international cloud infrastructure, and Ireland is the most commonly chosen EU jurisdiction for data centres by global technology companies, partly because of its favourable corporate tax regime.

[270] *See* NYU Compliance & Enforcement, *Is Foreign Bribery Jurisdiction an Element of Economic Sovereignty? Thoughts on Recent Policy Guidance from France and the U.S.* (May 15, 2020), https://wp.nyu.edu/compliance_enforcement/2020/05/15/is-foreign-bribery-jurisdiction-an-element-of-economic-sovereignty-thoughts-on-recent-policy-guidance-from-france-and-the-u-s/; *see also* Daskal, *Opening Salvo*, *supra* note 223, at 342 (discussing France's SecNumCloud certification framework as a mechanism for insulating sensitive data from U.S. CLOUD Act access).

commercial benefits. Nevertheless, China appears to prioritize data security and sovereign control over such commercial considerations.[271]

3. Reciprocity Mechanism

Finally, as discussed above, TAKE regulation face the greatest difficulty in avoiding blocking statutes through private international law mechanisms alone. The CLOUD Act therefore incorporates a reciprocity mechanism under which foreign states may obtain access through executive agreements concluded with the United States. In effect, this approach attempts to exchange defensive resistance for reciprocal benefits.

Although reciprocity agreements are formally public international law instruments, the concept of reciprocity is deeply familiar within private international law,[272] particularly in the recognition and enforcement of foreign judgments.[273]

In summary, extraterritorial data regulations do not operate in isolation. Rather, they interact with one another and frequently generate defensive responses. Together, they form an interconnected network of transnational data governance. Private international law is utilized not only in extraterritorial data regulation itself, but equally in the defensive mechanisms responding to such regulation. The more extensively private international law techniques are embedded within a regulatory framework, the more likely the framework can mitigate exposure to blocking statutes.

V. Conclusion

This article makes the following two major contributions. *First*, it identifies and analyzes the use of private international law in extraterritorial data regulation and demonstrates how private international law complements traditional forms of public regulation and enforcement. As the article has shown, different jurisdictions deploy private international law techniques differently, reflecting their respective regulatory priorities and strategic preferences. There is no inherently superior use of private international law. Rather, the effectiveness of such techniques depends upon their institutional and regulatory fit within the broader legal framework of each jurisdiction.

The United States represents the most aggressive approach among the three major jurisdictions examined in this article. Through the CLOUD Act, it has adopted an expansive form of TAKE regulation with significant extraterritorial reach. At the same time, the United States does not maintain a comprehensive blocking statute comparable to those found in the EU or China. This position is consistent with the reciprocal and outward-looking nature of the US approach. The United States encourages other jurisdictions to adopt similar standards and reciprocal arrangements in the TAKE context. This orientation is also broadly consistent with the traditional American vision of private international law. Despite historically expansive

[271] Latency is reduced when data is stored close to end users; Content Delivery Networks (CDNs) exploit this principle. Data localisation requirements may therefore require intermediaries to maintain local server infrastructure, increasing capital costs, or to forgo efficiency gains from centralised data processing.

[272] MOFCOM Rules art. 15.

[273] Many civil law countries—including China, France, Germany, and Japan—have traditionally required reciprocity for enforcing foreign judgments. *See* MOFCOM Rules art. 15 (treaty is an exception); Born & Rutledge, *supra* note 143, at 1017–19. Common law systems such as the United Kingdom and Singapore generally do not impose a reciprocity requirement.

assertions of judicial jurisdiction, US courts have generally been comparatively receptive toward the recognition and enforcement of foreign judgments.

China occupies the opposite end of the spectrum. While China has not, at least presently, adopted a TAKE statute comparable to the CLOUD Act, it has developed an extensive set of defensive mechanisms, including blocking statutes and data centralisation measures. This approach reflects China's preference for security, sovereign control, and regulatory autonomy, even where such measures may come at the expense of commercial efficiency and transnational data mobility.

The European Union occupies an intermediate position between these two approaches. The EU maintains blocking statutes, though generally in a less defensive form than China. At the same time, while the EU historically lacked a TAKE-style regime, recent developments show movement in that direction. Across all three jurisdictions, private international law techniques are utilized differently to advance the respective emphases underlying GIVE, USE, TAKE, and DEFENSE regulation.

Second, this article also contributes to the understanding of private international law itself. In particular, it demonstrates that extraterritoriality forms part of the private international law operational dynamics. The article further argues that traditional private international law justifications, especially party autonomy, may have become important justifications for certain forms of extraterritorial regulation, particularly through mechanisms such as submission clauses. At the same time, the article shows how blocking statutes, themselves deeply connected with private international law, may operate to police national assertions of jurisdiction and regulation that exceed the limits imposed by public international law.

Taken together, public international law and private international law form an interconnected hybrid system of checks and balances governing extraterritorial regulation among major powers such as the United States, the European Union, and China. This dynamic is especially visible in relation to data, given its increasing strategic, economic, and sovereign importance. It is hoped that this understanding of the interaction between private international law, public international law and extraterritoriality will facilitate future discussions of extraterritorial regulation beyond the context of data law.