UCI Law
UNIVERSITY OF CALIFORNIA, IRVINE SCHOOL OF LAW

The Foreign Sovereign Immunities Act in the Age of Transnational Surveillance: Judicial Interpretation and Legislative Solutions

By: Spencer Levitt and Andrea Cervantes
International Justice Clinic, University of California, Irvine School of Law

Published: August 21, 2023

Table of Contents

I. Executive Summary

In order to obtain jurisdiction over a foreign state in United States courts, litigants rely upon the statutory framework of the Foreign Sovereign Immunities Act of 1976 ("FSIA" or "the Act"). While the Act enumerates multiple exceptions to foreign sovereign immunity, the jurisprudential development of the "entire tort" doctrine in U.S. courts has effectively precluded jurisdiction against foreign sovereigns for transnational cyber espionage. This paper discusses the history of the Act and the development of the "entire tort" doctrine, argues that this approach runs counter to the text and purpose of the FSIA, and recommends a legislative solution to close the loophole which has granted foreign states immunity for conduct for which they should answer.

II. Introduction

The Foreign Sovereign Immunities Act provides the exclusive means of obtaining jurisdiction over a foreign sovereign in United States courts.[1] While the law on the books provides explicit exceptions to jurisdictional immunity—theoretically aiming to provide victims with effective redress against the tortious conduct of a foreign state—the common law development of the "entire tort" doctrine has hampered victims' ability to bring lawsuits. Federal courts have consistently held that, unless the "entire tort" takes place in the United States, the foreign state maintains immunity.[2] Drawn from the legislative history of the FSIA, a law enacted almost 50 years ago, this interpretation is grounded in the idea that torts are physical acts committed within a specific geographic area. But, this geographic interpretation no longer captures the reality of foreign state action.

Technological development has enabled covert and distanced intrusions which obscure the traditional understanding of how tortious conduct occurs. While technological torts have increased in recent years, no electronic privacy suit has been brought successfully against a foreign sovereign.[3] Jurisprudence has strayed too far from the intent of the FSIA and a clear exception is needed to effectively provide redress for victims of cyber torts. In order to reflect the intent behind the FSIA, U.S. courts should abandon the entire tort doctrine in favor of an analysis that understands how contemporary technology torts occur. This analysis would bring the United

---

[1] *See* 28 U.S.C. §§1602-1611 (1976). Congress has passed other statutes providing for jurisdiction in specific contexts. *See, e.g.,* Torture Victim Protection Act, 28 U.S.C. §1350 (1992); Genocide Accountability Act, 18 U.S.C. §1091(d) (2007); Torture Convention Implementation Act, 18 U.S.C. §§2340–2340A (1994); War Crimes Act of 1996, 18 U.S.C. §2441 (1996); Child Soldiers Accountability Act, 18 U.S.C. § 2442 (2008).

[2] Grayson Clary, Under the Foreign Sovereign Immunities Act, W*here do Hacking Torts Happen?*, Lawfare (May 1, 2018, 8:00 AM), https://www.lawfareblog.com/under-foreign-sovereign-immunities-act-where-do-hacking-torts-happen.

[3] Scott A Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to The Foreign Sovereign Immunities Act*, 46(3) Colum Hum. Rts. L. Rev. 227, 232 (2015).

States in line with a growing international trend.[4] Absent a judicial pivot, Congress should create an explicit carve-out so that victims of cyber torts can sue their assailants. Just as the passage of the FSIA served as a model for other state's sovereign immunity laws, it is again time for the United States to lead, or risk falling behind.[5]

III. The Pressing Issue

The proliferation of spyware tools in recent years has led to a surge in cross-border surveillance and cyber hacking that is "invisible-to-the-target".[6] Less than twenty years ago, these complex capabilities were only available to a handful of states.[7] However, a growing list of "pay-to-play" government customers have gained access to these invasive espionage technologies through the mercenary spyware industry.[8] Governments often use these tools to target political dissidents and political opponents, seeking to access their most private information. While cyber espionage may violate domestic privacy laws, lawsuits seeking redress

---

[4] Courts in the United Kingdom have endorsed a more reasonable interpretation of sovereign immunity, illustrating a potential path forward. In *Al Masarir v. Kingdom of Saudi Arabia*, the Royal Court of Justice held that Saudi Arabia could not assert a sovereign immunity defense against the Claimant (whose iPhones were allegedly infected with Pegasus spyware transmitted from the Saudi government). There, the Court relied on the plain meaning of the State Immunity Act of 1978 (SIA 1978), reasoning that the jurisdictional exception outlined in section 5 applies: (1) to both jure gestionis and jure imperri; and (2) the exception does not require that all of the alleged acts occurred in the United Kingdom, but only a causative act or omission. Similarily, *in Shehabi and Mohanned v. Kingdom of Bahrain*, the British High Court upheld jurisdiction against Bahrain for their deployment of FinSpy attacks against dissidents. Justice Knowles explained that section 5 of the SIA does not require "the presence of the infringing state actor in the UK... nor does it require all of the Defendant's acts to have occurred in the UK." Instead, Knowles noted that "it is enough if an at takes place in the UK which is more than a minimal cause of the injury".

[5] *See* Mark B. Feldman, *Foreign Sovereign Immunity in the United States Courts 1976-1986*, Vand. J. Transnat'l L. 19, 23 (1986) ("In fact, the FSIA has had a significant impact on international practice. The United Kingdom, Canada and several other countries have enacted statutes which apply the same basic principles as the FSIA.").

[6] Written testimony of John Scott-Railton, Senior Researcher, the Citizen Lab House Permanent Select Committee on Intelligence Hearing on "Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware", (July 27, 2022), https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-Scott-RailtonJ-20220727.pdf.

[7] *Id*.

[8] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, The Citizen Lab, (Sept. 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-co untries/.

against cyber attacks run into a critical procedural question: Can domestic courts extend jurisdiction over the foreign sovereign allegedly committing the tortious conduct?

In the United States, the 2017 case of *Doe v. Federal Democratic Republic of Ethiopia* grappled with this question. Kidane, a former citizen of Ethiopia, sought asylum in the United States after his government had grown increasingly hostile to dissent.[9] After becoming a naturalized citizen, he provided technical support to members of the Ethiopian diaspora who protested political corruption and human rights abuses occurring in Ethiopia.[10] Because of his activities, Kidane contended that the government of Ethiopia began surveilling him by deploying malware on his computer at his Maryland home.

The D.C. Circuit found that Kidane's claim was barred by sovereign immunity under the FSIA. Relying on the "entire-tort" doctrine, the Court held that two integral aspects of the tort occurred abroad—the "initial dispatch" of the malware and the "intent to spy".[11] As explained below, this narrow interpretation of the noncommercial tort exception runs afoul of the FSIA's plain language and the legislative intent underpinning the act. If this analysis is adopted by other circuits it will preclude redress for most tortious acts committed by foreign states.

IV. History of Foreign Sovereign Immunity in the United States

Until 1952, foreign states enjoyed near absolute sovereign immunity in the United States as a matter of comity.[12] This absolute theory of immunity was articulated in the historical 1812 U.S. Supreme Court case *The Schooner Exchange v. McFadden*, where Chief Justice Marshall reasoned that "[a]ll exceptions … to the full and complete power of a nation within its own territories, must be traced up to the consent of the nation itself."[13] Marshall's opinion was a fusion of two theoretical components.[14] It combined "syllogistic reasoning concerning the practices of nations" with "an inductive demonstration that the demands of the comity of nations … require recognition and application of the sovereign immunity concept."[15] These abstract theoretical principles reflect the "classic statement of the absolute theory of sovereign

---

[9] See Declaration of John Doe ("Kidane") in Support of Motion for Leave to Proceed in Pseudonym at ¶¶ 2–3, Doe v. Federal Democratic Republic of Ethiopia, No. 1:14-cv-372-CKK (D.D.C. Mar. 5, 2014), ECF No. 1-1, http://www.archive.org/download/gov.uscourts.dcd.165161/gov.uscourts.dcd.165161.1.1.pdf.
[10] *Id*, ¶¶ 4-6.
[11] *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7, 11 (D.C. Cir. 2017) ("Without the software's initial dispatch or an intent to spy—integral aspects of the final tort which lay solely abroad—Ethiopia could not have intruded upon Kidane's seclusion under Maryland law.").
[12] Judi L. Abbot, *The Noncommercial Torts Exception to the Foreign Sovereign Immunities Act*, 9(1) Ford. Int. L. Rev. 134 (1985).
[13] 11 U.S. 116, 136 (1812).
[14] Daniel T. Murphy, *The American Doctrine of Sovereign Immunity: An Historical Analysis*, 13 Vill. L. Rev. 583, 585 (1968).
[15] *Id*.

immunity."[16] That is, Courts will always dismiss actions against a foreign sovereign absent consent from the state. Following *Schooner*, U.S. courts embraced the idea that controversies over sovereign immunity should be dealt with by the executive branch, not the judiciary.[17]

In 1952, Department of State Legal Adviser Jack Tate thought a shift was required in US sovereign immunity law. The so-called "Tate Letter" argued that the classical approach to immunity, where states had to consent to jurisdiction, should be replaced by a "restrictive" approach. Tate explained that a foreign state's public acts (*acta jure imperri*) should be distinguished from their commercial or private acts (*acta jure gestionis*), where only the former should be afforded jurisdictional immunity.[18] Although issues of sovereign immunity remained under the executive's domain, the state department began to incorporate this restrictive approach in treaty negotiations with other nations.[19]

Inconsistent application of the restrictive theory, often informed by political considerations, necessitated a formalization of sovereign immunity law. In 1976 the FSIA was enacted.[20] The Act transferred primary responsibility for determining sovereign immunity from the executive branch to the judicial branch, making the United States the first state to codify foreign sovereign immunity into domestic law.[21] The Act defines a foreign state to include a "political subdivision" or an "agency or instrumentality of a foreign state".[22] Importantly, the FSIA does not include individual foreign officials, which is governed by extensive common law jurisprudence.[23]

While the FSIA makes foreign states presumptively immune from jurisdiction, several exceptions to immunity were included in accordance with the restrictive theory. Functioning as a

---

[16] *Id*. at 587.
[17] Abbot, *supra* note 4, at 135; *see also Republic of Mexico v. Hoffman*, 324 U.S. 30, 34 (1945) ("the national interests will be best served when controversies growing out of the judicial seizure of vessels of friendly foreign governments are adjusted through diplomatic channels rather than by the compulsion of judicial proceedings.")
[18] Simon G. Jerome, *Throwback Thursday: The Tate Letter and Foreign Sovereign Immunity, Transnational Litigation Blog* (May 26. 2022), https://tlblog.org/throwback-thursday-the-tate-letter-and-foreign-sovereign-immunity/.
[19] Abbot, *supra* note 4, at 136.
[20] *See* H.R. Rep. No. 1487, at 6606 ("A principal purpose of this bill is to transfer the determination of sovereign immunity from the executive branch to the judicial branch, thereby reducing the foreign policy implications of immunity determinations and assuring litigants that these often crucial decisions are made on purely legal grounds and under procedures that insure due process.").
[21] *See* Feldman, *supra* note 5, at 21; *Republic of Austria v. Altmann*, 541 U.S. 677, 691 (2004) (describing that the FISA "transfers primary responsibility for immunity determinations from the Executive to the Judicial Branch.").
[22] 28 U.S.C. §1603(a).
[23] *See, e.g., Samantar v. Yousuf,* 560 U.S. 305, 325 (2010) (holding that the FSIA does not govern foreign officials claims of immunity).

long-arm statute to establish jurisdiction, the FSIA provides for U.S. Court jurisdiction against a foreign sovereign if one of several exceptions is met.[24]

Section 1605 of the Act carves out these explicit exceptions to jurisdictional immunity, including the noncommercial tort exception, which states that a foreign state shall not be immune when:

> "money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment."[25]

When interpreting section 1605(a) "every federal court to have considered its scope has held that there is no jurisdiction unless the 'entire tort'—that is the tort *and* the injury—allegedly occurred inside the United States."[26]

Central to debates over the 'entire tort' theory is the meaning of and legislative intent behind the FSIA. In an early case favoring the theory, the court in *Matter of SEDCO* acknowledged in 1982 that Section 1605(a)(5) of the act was silent with respect to where the tort must occur for jurisdiction to exist, but relied on legislative history to find that "the tort, in whole, must occur in the United States."[27] There, the court cited the House Report accompanying the FSIA to note that the purpose of the Act was to "cover the problem of traffic accidents by embassy and government officials".[28] Two years later, D.C. Circuit Court Judge Harry Edwards disagreed with the reliance on the House Report in his concurrence in *Persinger v. Islamic Republic of Iran*. Judge Edwards emphasized that "the statute [Section 1605(a)(5)] plainly requires that *only the injury,* and not the tortious act or omission, occur in the United States… Congress never enacted the language of the House Report."[29] Even if the House Report is to be given deference, it is inconclusive because Congress merely refers to the jurisdiction of the United States, and not its territory.[30] While it is possible that Congress intended these to be one and the same, at the time of drafting, a more expansive interpretation of jurisdiction existed "including the principle that states have jurisdiction over acts that occur outside their territories but have an effect within their territories."[31]

---

[24] Feldman, *supra* note 4, at 22 n.14.
[25] 28 U.S.C. §1605(a)(5).
[26] John B. Bellinger III et. al, *Can You Be Sued Under the Foreign Sovereign Immunities Act?: A Primer for Foreign Governments and Their Agencies*, *Arnold & Porter* (Jan 26. 2021), https://www.arnoldporter.com/en/perspectives/advisories/2021/01/can-you-be-sued-under-fsia
[27] *Matter of SEDCO,* 543 F.Supp. 561, 567 (S.D. Tex. 1982).
[28] *Id.* (Citing H.R. Rep. *supra* note 9, at 6619).
[29] *Persinger v. Islamic Republic of Iran*, 729 F.2d 835, 844 (D.C. Cir. 1984); *see also Moskal v. U.S.* 498 U.S. 103, 108 (1990) ("In determining the scope of a statute, we look first to its language, giving the words used their ordinary meaning.") (internal quotation marks omitted).
[30] Stephen J. Schultze, *Hacking Immunity: Computer Attacks On United States Territory By Foreign Sovereigns*, 53 Am. Crim. L. Rev. 861, 869 (2016).
[31] *Id*.

More recent opinions have also relied on the Supreme Court's language in *Amerada Hess* describing "torts occurring within the territorial jurisdiction of the United States."[32] There, the Court relied on the principle of statutory construction that there should be a presumption against extraterritoriality when Congress does not explicitly note to which extraterritorial acts the clause should apply.[33] However, *Amerada Hess* does not resolve the issue of which parts of the tort or injury must occur in the United States because it dealt with property damage that was "unambiguously initiated and completed outside United States territory."[34]

The 'entire tort' interpretation has faced some judicial pushback. In the 1984 case of *Olsen ex rel. Sheldon v. Government of Mexico*, the Ninth Circuit held that subject matter jurisdiction existed over Mexico under the noncommercial tort exception.[35] In *Olsen*, a fatal plane crash in California was caused by many potentially tortious acts and omissions occurring in both the United States and Mexico.[36] While the court noted that section 1605(a)(5) "does not indicate that the conduct causing the tort must also take place in the United States," the court also recognized that the legislative history of the FSIA might indicate otherwise.[37] To analyze which aspect of the tortious conduct ought to occur in the United States for there to be jurisdiction, the opinion contrasted the *SEDCO* case. In *SEDCO*, jurisdiction was denied because "*none* of the alleged acts or omissions… occurred in the United States."[38] Conversely, the court in *Olsen* held that, because conduct constituting a single tort occurred in the United States (the negligent piloting of the aircraft) the noncommercial tort exception applied.[39] Supporting their holding, the court emphasized the perverse incentive created by an overly-broad interpretation of the "occuring in the United States" language from 1605(a) of the Act—it encourages artful pleading on the part of foreign states.[40] Holding otherwise would "contradict the purpose of the FSIA, which is to 'serve the interests of justice and … protect the rights of both foreign states and litigants in United States courts.'"[41]

Whether just the injury has to occur in the United States or a broader scope encompassing every aspect of the tort is necessary has significant bearing on findings of jurisdiction under the noncommercial exception. But merely relying on the language and intent of a law passed nearly 50 years ago may be a futile effort. "At the time of passage in 1976, it is possible that Congress

---

[32] *Id. at* 869-873 (2016).
[33] *See Argentine Republic v. Amerada Hess Shipping Corp*., 488 U.S. 428 (1989)).
[34] Schultze, *supra* note 28, at 870.
[35] *Olsen ex rel. Sheldon v. Government of Mexico*, 729 F.2d 641 (9th Cir. 1984).
[36] *Id*. at 645-646.
[37] *Id*. at 645.
[38] *Id.* at 646 (citing *Matter of SEDCO*, 543. F.Supp. 561, 567 (S.D. Tex. 1982)).
[39] *Id*.
[40] *Id.* ("By requiring every aspect of the tortious conduct to occur in the United States, a rule such as in *SEDCO* would encourage foreign states to allege that some tortious conduct occurred outside the United States. The foreign state would thus be able to establish immunity and diminish the rights of injured persons seeking recovery.")
[41] *Id*. (quoting 28 U.S.C. §1602).

simply did not anticipate acts or omissions with significant cross-border effect."[42] Instead, a solution is needed to encompass the surge in cross-border cyber torts.

V. Sovereign Immunity and Cyber Torts

As technology has created an interconnected world, state actors are reaching across borders to stifle dissent, intimidate critics, and hack their targets.[43] The FSIA was enacted prior to contemporary capabilities that have enabled the deployment of sophisticated digital tools over the internet.[44] Section 1605(a)(5) of the Act requires the injury complained of to occur in the United States for the jurisdictional exception to apply, but it does not indicate whether the conduct causing the tort, or setting into motion, must also take place in the United States.[45] The new frontier of technological torts complicates this analysis. Determining which actions preceding an injury constitute aspects of the tortious conduct, and drawing a line for which of these actions must occur within a single sovereign territory to constitute the entire tort, is a mushy and practically metaphysical task. But this process is exactly what has been endorsed by the jurisprudential development of the 'entire tort' doctrine. Rather than focusing on where substantial parts of the act and injury occur—as courts generally have done when analyzing cross-border torts generally—the entire tort analysis under the FSIA is an anomaly.[46]

In the context of cyber torts, determining where the aspects of the tort occur becomes more difficult. *Doe v. Federal Democratic Republic of Ethiopia ("Kidane")* applied an expansive scope of the entire tort doctrine. There, the D.C. Circuit rejected jurisdiction for the plaintiff's claim that the Ethiopian government deployed malware on his computer at his Maryland home.[47] The Court held that two integral aspects of the tort occurred abroad—the "initial dispatch" of the malware and the "intent to spy."[48] To counter this point, the plaintiff analogized two cases that involved assassinations originating from foreign states: *Liu v. Republic of China*[49] and *Letelier v. Republic of Chile*.[50] In both of these cases, although the attacks were "planned, commanded, or directed" abroad, they involved actions in the United States that were considered tortious without any connection to the action taken abroad.[51]

---

[42] Schultze, *supra* note 28 at 869.
[43] Gilmore, *supra* note 3, at 229.
[44] *See, e.g., Id.* at 231 ("Decades ago, this sort of spying on U.S. targets would have required physically bugging offices and tapping phone lines.").
[45] Olsen, 729 F.2d at 645.
[46] Gilmore, *supra*. at 254 n.134.
[47] Doe, 851 F.3d 7.
[48] *Id.* at 11.
[49] 892 F.2d 1419 (9th Cir. 1989).
[50] 488 F.Supp. 665 (D.D.C. 1980).
[51] "D.C. Circuit Finds Ethiopia Immune in Hacking Suit," 131 Harv. L. Rev. 1179, 1182 (2018) (quoting Final Reply Brief of Appellant at 5, *Doe*, 851 F.3d 7, https://www.eff.org/files/2017/01/03/12.27.16_final_reply_brief_of_appellant_john_doe.pdf

Nonetheless, the Court in *Kidane* read an intent requirement into the noncommercial exception of the FSIA. This requirement departs from the plain language of the Act and the precedents of other circuits.[52] This requirement is also in opposition to a growing body of international law.

Additionally, by requiring that the initial dispatch of the attack occur within U.S. territory, the entire tort rule reifies the Ninth Circuit's concern in *Olsen* that an expansive territorial requirement encourages gamesmanship on behalf of the sovereign subject to suit.[53] The temporal ambiguity surrounding when intent is formed and which acts precipitated the tort are inexact, and "future courts are left to guess what standard *Kidane* applied in choosing to incorporate transmission into the 'entire tort.'"[54]

Moreover, the court selectively applied the text, legislative history, and drafter's intent behind the FSIA to reach its conclusion. Writing that the Act was only intended to apply to a narrow scope of tortious conduct, the court referenced the Act's purpose of eliminating traffic accidents.[55] Yet, reading beyond Section 1605(a)(5)'s requirement of an "injury… occurring in the United States," the D.C. Circuit required that the "initial dispatch" and "intent to spy" also occur in the United States. The D.C. Circuit should have stuck strictly to the text of the FSIA in accordance with the principles of statutory interpretation. As Mark B. Feldman—former Deputy Legal Advisor at the Department of State who was deeply involved in the drafting of the FSIA—stated: "The whole point of the FSIA is that, going forward, any sort of immunity defense made by a foreign sovereign in an American court must stand on the Act's text. Or it must fall."[56]

Construing the FSIA to create a high bar for bypassing immunity facilitates the proliferation of cyber attacks. If more circuits follow this approach, the remedial purpose of the FSIA will be rendered moot.

VI. Arguments for a Judicial Interpretation of a Cyber Tort Exception

As cross-border surveillance and cyber espionage increase at the hands of foreign states, victims in the United States will continue to lack remedy against state actors for such serious privacy violations so long as the 'entire tort' doctrine drives FSIA analysis of such cases. To avoid that outcome, courts should reconsider the doctrine when it comes to the interpretation of section 1605. Luckily, desirable replacements already exist. As one practitioner and observer has

---

[52] *Id.* at 1183.
[53] *See Olsen*, 729 F.2d 641.
[54] 131 Harv. L. Rev., *supra* note 28, at 1185.
[55] *Doe, supra* note 24, at 11 (quoting *Argentine Republic v. Amerada Hess Shipping Corp*., 488 U.S. 428, 439-40 (1989)).
[56] Mark B. Feldman, "A Drafter's Interpretation of the FSIA," *American Bar Association Section of International Law*, Winter 2018, https://www.foster.com/assets/htmldocuments/pdfs/ABA-ACHL-Newsletter-Winter-2018.pdf

noted, "We need only apply the old laws of immunity and tort to the new frontier of cyberspace."[57]

A. Effects Tests

The 'entire tort' requirement departs from a focus on effects in both civil and criminal cases analyzing other jurisdictional issues of cross-border cyber activity.

In the context of personal jurisdiction between U.S. states, the California Supreme Court held that an individual's knowledge that harm will likely be suffered in a forum state, combined with evidence of express aiming or intentional targeting of that state, is sufficient to find personal jurisdiction in the state where the harm occurred.[58] This same principle is expressed in U.S. criminal law. In *United States v. Ivanov*, the court found jurisdiction "because the intended and actual detrimental effects of Ivanov's actions in Russia occurred within the United States."[59] There, although the hacker was located in Russia, because he targeted a Connecticut based corporation with the cyber attack, there existed jurisdiction.[60] Supporting this principle is the inverse case of the *U.S. v. Vasiliy Vyacheslavovich Gorshkov*, where although the hackers were located in the United States, because the computer targeted was located in Russia, there was no harm within the United States leading the Court to deny jurisdiction.[61]

Focusing on the effect of the attack reflects established principles of private international law. If an attacker intends to cause effects within a foreign state, they have availed themselves to jurisdiction in that state.[62] This reasoning has been endorsed by courts in the United Kingdom, particularly in the context of sovereign immunity for cyber torts. For example, in *Al Masarir v. Kingdom of Saudi Arabia*, the Royal Court of Justice held that Saudi Arabia could not assert a sovereign immunity defense against the Claimant (whose iPhones were allegedly infected with Pegasus spyware transmitted from the Saudi government). The court relied on the plain meaning of the State Immunity Act of 1978 (SIA 1978), reasoning that the jurisdictional exception outlined in section 5 applies: (1) to both jure gestionis and jure imperii; and (2) the exception does not require that all of the alleged acts occurred in the United Kingdom, but only a causative act or omission.[63]

U.S. courts can also work on the "presumption that someone can be present abroad through cyberspace."[64] Adopting this approach reflects the reality of cyber torts, emphasizing

---

[57] Gilmore, *supra* note 3, at 233.
[58] *See Pavlovich v. Superior Court*, 29 Cal.4th. 262, 273 (2002).
[59] 175 F.Supp.2d 367, 370 (D. Conn. 2001).
[60] *Id.* at 371 ("The fact that the computers were accessed by means of a complex process initiated and controlled from a remote location does not alter the fact that the accessing of the computers, i.e. part of the detrimental effect prohibited by the statute, occurred at the place where the computers were physically located…").
[61] No. CR00-550C, 2001 WL 1024026 (W.D. Wash. 2001).
[62] Kristin Carlberg, *Suing a State for Cross-border Cyber Torts? Overcoming the Immunity of the Hacking State*, Orebro University, 20 n.128-129 (2017).
[63] Al-Masarir v. Kingdom of Saudi Arabia [2022] EWHC 2199.
[64] Carlberg, *supra* note 62, at 19.

that if an actor can have an effect in a particular place, they necessarily have availed themselves to that forum. Conversely, requiring the physical presence of the attacker within the territory where the injury occurs relies on an outdated conception of tortious conduct. "Such an inflexible requirement," one observer noted, "will become unworkable as technology lowers the barrier to cross-border injuries of various types."[65] According to Gilmore, "[c]ourts should see cyber intrusions for what they are: the functional equivalent of physical trespass within the United States."[66]

B. Substantial Portion Tests

Tests focusing on where a substantial portion of the tortious conduct occurred have also been applied by U.S. courts in the context of foreign sovereign immunity.[67] These tests provide a more workable standard by allowing Courts to locate the gravemen of the tort without engaging in the esoteric task of tracking an offense from its inception to its conclusion. While determining whether a "substantial portion" of a tort will in some cases require delving into complex questions of what ultimately counts, this fact-finding is precisely what courts exist to determine. Furthermore, the common law provides crucial guidance for courts in applying the substantial portion test, as cases like *Liu*, *Olsen*, *Asociacion*, and *Letelier* demonstrate.

For instance, in the case of *Letelier v. Republic of Chile*, the Chilean government was accused of assassinating a diplomat in the United States.[68] Although "there is no doubt that the precipitating acts were extraterritorial, [because] the consummation and injury were within the United States" the Court found jurisdiction.[69] This principle was echoed in *Asociacion de Reclamantes v. United Mexican States*. There, the D.C. Circuit held that the noncommercial tort exception under section 1605 did not apply because the "essential locus" of the tort occurred outside of the United States.[70] In that case, because the plaintiff's claims against Mexico alleged breach of a claims-settlement treaty, and because the decision to breach that treaty was made entirely in Mexico, the "essential locus" was not in the United States. Similarly, in *Olsen*, the Ninth Circuit held that "at least one entire tort occurring in the United States" is needed to have jurisdiction under the noncommercial tort exception.[71] Deploying a substantial portion approach enables Courts to segment tortious conduct into identifiable portions, such as where and how the injury occurred.

---

[65] Schultze, *supra* note 23, at 876.
[66] Gilmore, *supra* note 3, at 258.
[67] For a thorough discussion about various substantial portion tests, *see* Gilmore, *supra* note 3, at 253-256.
[68] *Liu*, 892 F.2d 1419.
[69] Schultze, *supra* note 23, at 876.
[70] Asociacion de Reclamantes v. United Mexican States, 735 F.2d 1517, 1525 (D.C. Cir. 1984).
[71] *Olsen*, 729 F.2d at 646.

Finding otherwise would be against the FSIA's purpose of serving the interests of justice and protecting the rights of litigants.[72] As noted by Joseph W Dellapenna, a member of the ABA working group on the FSIA, "if a country plotting a political murder in the United States were to take steps to ensure that some small part of the wrongful act … took place abroad, no suit could be brought against the responsible foreign state in the United States."[73] A similar substantial portion test should be applied to cyber torts; a more expansive approach mistakes contemporary cyber torts with physical intrusions, giving foreign states leeway to evade suits.

C. Criminal Exception

Another avenue for redress, falling outside the FSIA, is through criminal prosecution. Traditionally, scholars and courts alike have accepted that "the FSIA provides the sole basis for obtaining jurisdiction over a foreign state in federal court."[74] However, Professor Chiméne Keitner argues that this is only true in the civil context; the FSIA is inapplicable to criminal proceedings.[75] Until Congress explicitly acts, jurisdiction over a foreign sovereign in criminal proceedings will remain a matter of common law.[76] Although foreign states are generally incapable of incurring criminal liability under U.S. domestic law, the same cannot be said for state-owned enterprises ("SOE").[77] To this end, any act of cyber surveillance or espionage by an "agency or instrumentality" of a foreign state should be subject to criminal jurisdiction in U.S. courts under the commercial activity exception of Section 1605 of the Act.[78]

Another avenue is through 18 U.S.C. §3231 which may confer criminal jurisdiction over the instrumentalities of foreign sovereigns. Under this statute, "district courts of the United States shall have original jurisdiction, exclusive of the courts of the States, of all offenses against the laws of the United States."[79] Only this year the Supreme Court, in *Turkiye Halk Bankasi A.S. v. United States*, rejected a Turkish bank-petitioner's arguments and found that §3231 provides

---

[72] Olsen, *supra* note 40.

[73] Joseph W. Dellapenna, *Refining the Foreign Sovereign Immunities Act*, 9 Willamette J. Int'l & Dis. Res. 57, 137 (2001).

[74] Argentine Republic v. Amerada Hess Shipping Co., 488 U.S. 428, 439 (1989).

[75] *Turkiye Halk Bankasi A.S. v. United States*, 598 U.S. __, 5 (2023) ("the Act does not provide foreign states and their instrumentalities with immunity from *criminal* proceedings") (emphasis in original). *See also* Chiméne Keitner, *Prosecuting Foreign States*, 61 Va. J. Int'l. L. 221 (2021).

[76] *Id.*

[77] *Id.* at 267-268; *see also* Curtis Bradley and Jack Goldsmith, *Turkiye Halk Bankasi A.S. v. United States, Part 1: The FSIA and Criminal Prosecutions*, Lawfare (Jan. 11, 2023, 8:31 AM), https://www.lawfareblog.com/turkiye-halk-bankasi-v-united-states-part-1-fsia-and-criminal-prosecutions (noting that the United States is arguing that the FSIA only applies to civil actions).

[78]

[79] Keitner, *supra* note 75, at 268 ("By contrast, separate entities such as SOEs and other agents of foreign states are subject to domestic criminal jurisdiction, at a minimum, for their commercial activities under the restrictive theory, and perhaps for other acts that violate U.S. criminal law.").

federal courts with criminal jurisdiction over state instrumentalities and that the FSIA does not apply to criminal proceedings against states or their instrumentalities.[80]

VII. Supporting a Legislative Carve-Out

Absent a correction of jurisprudence on the whole tort doctrine, legislation should expressly grant courts jurisdiction over states that use spyware against a person in American territory. This approach would reflect United States law in other areas where exceptions to sovereign immunity are made for certain state-sponsored human rights abuses. Creating a legislative carve-out ensures that at least in some circumstances, foreign states cannot freely abuse US laws with impunity.

In this section, we will first examine the Justice Against Sponsors of Terorrism Act which may provide a model to address cross-border cyber torts in U.S. courts. Second, we will highlight some of the concerns raised about further restrictions to sovereign immunity. The included Annex proposes draft legislation, offering language that could be used in an amendment to the FSIA to include concrete sovereign immunity exceptions in cases of torts linked to human rights abuses caused by state-sponsored cyber espionage.

Despite reservations raised by some that such legislative change would inconvenience national interests abroad by supporting reciprocal jurisdiction against the United States, these issues could be addressed by strict limitation on the use of such technologies by the United States. The Biden administration's recent executive order does in fact place heavy restrictions on the use of commercial spyware, used in a variety of different contexts.[81] Regardless, the grave threat to privacy posed by state-sponsored digital surveillance supports such a change to sovereign immunity. It is essential to provide some remedy for victims and add legal pressure to state abusers to halt such attacks.

A. The Justice Against Sponsors of Terrorism Act

In an attempt to provide victims of terrorist attacks with a judicial remedy, Congress passed the Justice Against Sponsors of Terrorism Act ("JASTA"). The act provides that victims of state-sponsored terrorism may sue foreign governments in U.S. courts for monetary damages. This exception was adopted in the aftermath of the September 11 attacks and created a path for victims and their families to file suit against states, namely Saudi Arabia.[82] It has enabled

---

[80] *Turkiye Halk Bankasi A.S., supra* at 3 - 5.

[81] Exec. Order, Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, (2023), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/.

[82] Curtis Bradley & Jack Goldsmith, *Don't Let Americans Sue Saudi Arabia*, New York Times (Apr. 22, 2016), https://www.nytimes.com/2016/04/22/opinion/dont-let-americans-sue-saudi-arabia.html

Americans to successfully sue foreign sovereigns for harms related to state-sponsored terrorism around the world.

Congress, by drafting JASTA, acknowledged the procedural hurdle existing under the FSIA. Providing a specific exception for state-sponsored terrorism, the bill does the following:[83]

> "authorizes federal court jurisdiction over a civil claim against a foreign state for physical injury to a person or property or death that occurs inside the United States as a result of: (1) an act of international terrorism, and (2) a tort committed anywhere by an official, agent, or employee of a foreign state acting within the scope of employment."

The bill also provides for civil liability on a person who conspires to commit or aids or abets terrorism, and applies to civil claims arising on or after September 11, 2001. Relatedly, for some federal crimes, Congress has prescribed jurisdiction against individuals who committed crimes that often implicate foreign state actions.[84] The language from JASTA, or from one of these individually focused statutes, serve as a useful model for a potential carve-out for cyber espionage.

B. Reservations About Legislative Change

Critics of JASTA have raised several concerns that would likely apply to a legislative proposal to grant a legislative carve out in the case of a cyber tort. However, by narrowly constructing a sovereign immunity exception to apply solely to cross-border cyber torts, Congress can effectively provide relief for victims of spyware while limiting the potential risks—just as JASTA aimed to do.

i. Concerns that Exceptions Set Dangerous Precedence for the U.S. Do Not Apply in the Context of Sovereign Immunity

Critics of JASTA, including President Obama, who vetoed the bill, highlight three concerns that support not allowing victims to pursue legal remedy in U.S. Court. First, they argued that such a measure inappropriately shifts the power of diplomatic relations to the judiciary and away from its proper place in the executive. However, in the context of sovereign immunity, this concern was outwardly rejected by the passage of the FSIA. The FSIA explicitly shifted authority over sovereign immunity from the executive to the judiciary.[85]

Second, critics argued that such an exception jeopardizes U.S. interests abroad by encouraging greater suits against the U.S. as sovereign. However, as noted above, the recent Executive Order responds to this concern, explicitly limiting the United States from using commercial spyware.[86] Additionally, this reciprocity concern always exists in discussions about

---

[83] Justice Against Sponsors of Terrorism Act (JASTA), Pub. L. No. 114-222, 130 Stat. 852 (2016).

[84] *See* Torture Victim Protection Act, 28 U.S.C. § 1350 (2018); Genocide Accountability Act of 2007, 18 U.S.C. § 1091(d) (2018); War Crimes Act of 1996, 18 U.S.C. § 2441 (2018); Child Soldiers Accountability Act of 2008, 18 U.S.C. § 2442 (c) (2018)

[85] *See Republic of Austria*, *supra* note 20.

[86] The White House, *Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security* (Mar. 27, 2023)

broadening jurisdiction, yet it is essential for individuals in the United States to have some recourse to surveillance conducted against them.

Supporters argued that because JASTA supplied victims with a necessary remedy, and did so through narrow means, its benefits outweighed the risks.[87] Even if one does not take that position with respect to JASTA, the argument holds true for a legislative amendment to the FSIA. In supporting JASTA's override of President Obama's veto, Senator Ben Cardin acknowledged the potential for unintended consequences abroad, but concluded that "the risk of shielding the perpetrators of terrorism from justice outweighs the risks on how other countries might respond to and perhaps compromise U.S. interests."[88] In a similar vein, it is necessary for Congress to adopt a narrow exception for cyber torts so that victims of foreign espionage can be made whole, while interests of national security are simultaneously upheld.

Annex:
Sample Proposal for Draft Legislation for Cyber Tort Exception to Foreign Sovereign Immunity

A. Proposed Addition to US Code: 28 U.S.C. 1605

(a) A foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case—

> (1) not otherwise covered by this chapter in which money damages are sought against a foreign state for personal injury that was caused by a use of intrusion software to surveil an individual through an electronic device, where a substantial portion of the tort occurs within the territory of the United States, if such act or provision of material support or resources is engaged in by an official, employee, or agent of such foreign state while acting within the scope of his or her office, employment, or agency.

---

https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/ ("Therefore, I hereby establish as the policy of the United States Government that it shall not make operational use of commercial spyware that poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person.").

[87] The bill has "a narrow focus that only allows suits against foreign governments—not individuals like diplomats or military troops, as critics claim." John Cornyn & Terry Strada, *No Remorse for Passing the Needed Jasta Act*, Wall Street Journal, Oct. 9, 2016.

[88] Press Release, Ben Cardin, U.S. Senator, Floor Speech on the Veto Override of the Justice Against Sponsors of Terrorism Act (JASTA), (Sept. 28, 2016), https://www.cardin.senate.gov/press-releases/floor-speech-on-the-veto-override-of-the-justice-against-sponsors-of-terrorism-act-jasta/.

(2) Definitions.—The term "intrusion software"[89] is defined as software specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network capable device, and performing any of the following:

(A) The extraction of data or information, from a computer or network capable device, or

(B) the modification of system or user data; or

(C) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

[89] We used the definition of intrusion software under § 772.1 Definitions of terms as used in the Export Administration Regulations (EAR), 15 CFR 772.1, https://www.ecfr.gov/current/title-15/section-772.1. The definition of intrusion software needs further examination.