Extinguishing the Firewall: Addressing the Jurisdictional Challenges to Bringing Cyber Tort Suits Against Foreign Sovereigns

The rapid advancement of technology has resulted in new forms of tortious activity. Increasingly, these cyber torts are perpetrated by foreign states. Notwithstanding other barriers to collecting damages for a cyber tort, a plaintiff suing for a foreign-state-perpetrated cyber tort must prove that the alleged tortious activity satisfies one of the Foreign Sovereign Immunities Act's exceptions—most likely the noncommercial tort exception. Recently the U.S. Court of Appeals for the D.C. Circuit held that a U.S. court lacked jurisdiction to hear a claim against a foreign state that hacked a U.S. national's email account. The court found the noncommercial tort exception inapplicable because the intent to hack was held by a party abroad, and thus the "entire tort" did not occur in the United States. This Note argues that the D.C. Circuit improperly extended the "entire tort" doctrine from traditional physical torts to cyber torts. Instead, the noncommercial tort exception should apply to foreign-state-perpetrated cyber torts. This Note further proposes a modified location test for courts to use in determining whether a cyber tort satisfies the exception's "occurring in the United States" requirement.

INTRODUCTION

We live in an age in which technology is constantly evolving. From the invention of email in 1978,[1] to the launch of the first iPhone in 2007,[2] to the introduction of an autopilot-equipped Tesla automobile in 2015,[3] technology is undoubtedly advancing at a rapid rate. It is no surprise that these and other advances in technology have coincided with novel forms of unlawful activity. In the past five years, cyber torts—tortious activity primarily conducted through cyberspace—have occurred with alarming frequency against a wide variety of victims,

1. Doug Aamoth, *The Man Who Invented Email*, TIME (Nov. 15, 2011), http://techland.time.com/2011/11/15/the-man-who-invented-email/ [https://perma.cc/4MJF-48JS].

2. Juli Clover, *10 Years Ago Today, the Original iPhone Officially Launched*, MACRUMORS (July 29, 2017, 7:05 AM), https://www.macrumors.com/2017/06/29/iphone-10-years/ [https://perma.cc/HU4E-RZ52].

3. *Your Autopilot Has Arrived*, TESLA (Oct. 14, 2015), https://www.tesla.com/blog/your-autopilot-has-arrived [https://perma.cc/ZU26-XHC6].

including Equifax,[4] the U.S. Securities and Exchange Commission,[5] and, perhaps most infamously, the 2016 U.S. presidential election.[6] Indeed, the Democratic National Committee ("DNC") recently filed suit against the Russian Federation for its role in hacking the DNC's servers during the 2016 presidential election.[7]

Although high-profile cyber torts garner the most media attention, smaller, targeted hacks also have the potential to inflict significant damage. In June 2017, a single entity hacked DLA Piper,[8] Merck, and Heritage Valley Health Systems, among others.[9] Critically, the hack of Heritage Valley Health Systems impaired the functioning of some hospital equipment.[10] Thankfully, the system impairment at Heritage Valley did not result in the loss of life; however, such grievous consequences are not outside the realm of possibility, especially given health care's increasing reliance on technology.[11]

---

4. Jamie McGee, *Nearly Half of Tennessee Residents Affected by Equifax Breach, AG Says*, TENNESSEAN (Sept. 19, 2017, 4:43 PM), http://www.tennessean.com/story/money/2017/09/19/equifax-breach-tennessee-slatery-letter-security/682794001/ [https://perma.cc/L99B-9H4H].

5. Sarah N. Lynch & Dustin Volz, *Hack of Wall St Regulator Rattles Investors, Lawmakers*, REUTERS (Sept. 21, 2017, 11:07 AM), https://www.reuters.com/article/legal-sec-cyber/hack-of-wall-st-regulator-rattles-investors-lawmakers-idUSKCN1BW2AY [https://perma.cc/W2HQ-LZQV].

6. *Russian Hacking and Influence in the U.S. Election*, N.Y. TIMES, https://www.nytimes.com/news-event/russian-election-hacking (last visited Dec. 13, 2018) [https://perma.cc/7UVF-9CCD] [hereinafter *Russian Hacking Coverage*].

7. Complaint, Democratic Nat'l Comm. v. Russian Federation, No. 1:18-cv-03501-JGK (S.D.N.Y. Apr. 20, 2018), 2018 WL 1885868; *see also* Jury Demand & Amended Complaint, Democratic Nat'l Comm. v. Russian Federation, No. 1:18-cv-03501-JGK (S.D.N.Y. Oct. 3, 2018).

8. Debra Cassens Weiss, *DLA Piper Hit by 'Major Cyber Attack' amid Larger Hack Spreading to US*, A.B.A. J. (June 27, 2017, 12:27 PM), http://www.abajournal.com/news/article/dla_piper_is_hit_by_major_cyber_attack_amid_larger_hack_spreading_to_us [https://perma.cc/7EA4-QQH7].

9. Chris Mondics, *Merck Hack Part of a Massive Global Attack*, PHILA. INQUIRER (June 27, 2017, 11:32 AM), http://www.philly.com/philly/business/merck-is-the-target-of-a-massive-hack-20170627.html [https://perma.cc/25KT-K8WQ]; Chelsea Simeon, *Heritage Valley Health System Hit by 'Widespread' Cyber Attack*, WKBN FIRST NEWS 27 (June 27, 2017, 2:54 PM), https://www.wkbn.com/local-news/heritage-valley-health-system-hit-by-widespread-cyber-attack/1067722397 [https://perma.cc/DU3Y-H7W8].

10. Simeon, *supra* note 9; *see also Heritage Valley Health, Drugmaker Merck Hit by Global Ransomware Cyberattack*, PITTSBURGH POST-GAZETTE (June 27, 2017, 11:30 AM), http://www.post-gazette.com/business/tech-news/2017/06/27/Heritage-Valley-Health-Merck-targets-cyberattack-pennsylvania-ransomware/stories/201706270148 [https://perma.cc/DP23-974G] (discussing the operational slowdowns resulting from the hack, which necessitated the rescheduling of surgical procedures).

11. *See* David Goldman, *A Hacker Can Give You a Fatal Overdose*, CNN (June 10, 2015, 11:31 AM), https://money.cnn.com/2015/06/10/technology/drug-pump-hack/index.html [https://perma.cc/2YCQ-9TNX] (noting story of Billy Rios, an independent security researcher, who "discovered the potentially much more dangerous vulnerability: A hacker could purposefully give a patient a fatal overdose"); *see also Heritage Valley Health "Working to Determine" Whether Patient Information Stolen in Cyber Attack*, PITTSBURGH'S ACTION NEWS 4, https://www.wtae.com/article/cybersecurity-incident-heritage-valley-health-system/10228015 (last updated June 28, 2017, 6:00 PM) [https://perma.cc/3L2P-7LH9] (discussing how the hospital continued with some surgeries, though others were postponed); *Updates on the Cyber Security Incident at Heritage Valley Health*

More commonly, hacks cause severe economic damage. The insurance market Lloyd's of London estimates that economic damage from a single "serious cyber-attack" could total more than $120 billion.[12] Moreover, in 2016 alone, "cybercrime cost the global economy over $450 billion, over 2 billion personal records were stolen and in the U.S. alone over 100 million Americans had their medical records stolen."[13] As these examples show, damaging and unlawful cyberactivity is becoming increasingly commonplace—already affecting billions of victims.[14]

Given the increased use of cyberspace to commit unlawful activity, it comes as no surprise that foreign states are also using cyberspace to conduct illicit activities. Numerous countries have recently been connected to high-profile cyber torts, including the United States' monitoring of communications from high-level foreign officials such as German chancellor Angela Merkel;[15] the North Korean hack of Sony Pictures;[16] and Russian interference with the 2016 U.S. presidential election,[17] the 2017 French election,[18] and the 2018 Winter Olympics.[19] These incidents raise two important questions: What legal framework applies to cyber torts, and how can victims seek redress for cyber torts perpetrated by foreign states?

System, HERITAGE VALLEY HEALTH SYS., http://www.heritagevalley.org/news_posts/updates-on-the-cyber-security-incident-at-heritage-valley-health-system (last updated July 3, 2017, 7:25 PM) [https://perma.cc/G72A-DR9K] (mentioning the challenge in providing care without access to computers).

12. Julia Kollewe, *Lloyd's Says Cyber-attack Could Cost $120bn, Same as Hurricane Katrina*, GUARDIAN (July 17, 2017, 2:03 AM), https://www.theguardian.com/business/2017/jul/17/lloyds-says-cyber-attack-could-cost-120bn-same-as-hurricane-katrina [https://perma.cc/S4MY-7LUQ].

13. Luke Graham, *Cybercrime Costs the Global Economy $450 Billion: CEO*, CNBC (Feb. 7, 2017, 10:00 AM), https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html [https://perma.cc/K8VX-Q2HC] (quoting Steve Langan, chief executive at Hiscox Insurance).

14. *See id.* (noting that amid an " 'epidemic of cybercrime' . . . [c]ompanies are increasingly factoring cyber-attacks into their business").

15. James Ball, *NSA Monitored Calls of 35 World Leaders After US Official Handed over Contacts*, GUARDIAN (Oct. 25, 2013, 2:50 AM), https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls [https://perma.cc/9JPB-UYQU].

16. David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES (Dec. 17, 2014), https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html [https://perma.cc/FK7J-CG8Y].

17. *Russian Hacking Coverage*, *supra* note 6.

18. Andy Greenberg, *The NSA Confirms It: Russia Hacked French Election 'Infrastructure,'* WIRED (May 9, 2017, 12:36 PM), https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/ [https://perma.cc/38VT-HWHZ].

19. Ellen Nakashima, *Russian Spies Hacked the Olympics and Tried to Make It Look Like North Korea Did It, U.S. Officials Say*, WASH. POST (Feb. 24, 2018), https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html [https://perma.cc/9KSC-VRMC].

Because cyber torts do not perfectly conform to traditional legal parameters, courts have had to adapt and reinterpret current laws in order to provide victims with a judicial avenue through which they can hold perpetrators of cyber torts accountable.[20] In their empirical study of cyber tort litigation, Professors Michael Rustad and Thomas Koenig identified "traditional causes of action modified or reshaped significantly by the Internet" as one of many phenomena brought on by cyber torts.[21] This Note focuses on those, answering whether cyber tort victims can seek legal redress for foreign-state-perpetrated cyber torts and, if so, how.

Central to this inquiry is determining whether foreign states are entitled to sovereign immunity for cyber torts. Foreign sovereign immunity precludes individuals from bringing civil suits against foreign states absent particular allowances.[22] In the United States, victims may seek civil redress from a foreign state only if the state's activity falls within one of the general exceptions to the Foreign Sovereign Immunities Act of 1976 ("FSIA")[23] or a targeted exception to the FSIA, such as the recently passed Justice Against Sponsors of Terrorism Act ("JASTA").[24] If a foreign state's action falls under an exception to the FSIA, immunity does not apply, and the FSIA confers jurisdiction over the action to U.S. courts.[25] Most state-perpetrated cyber torts appear to fall most naturally under the noncommercial tort

---

20. *See generally* Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 77 (2003) ("[T]he rise of a new technology requires courts to stretch traditional tort doctrines as well as to create updated torts to keep pace with new civil wrongs."); Paul Rosenzweig, *When Companies Are Hacked, Customers Bear the Brunt. But Not for Long.*, NEW REPUBLIC (Oct. 15, 2013), https://newrepublic.com/article/115187/cybersecurity-liability-court-cases-are-changing-blame-game [https://perma.cc/DC2N-MCEH]:

> Legal developments in [the cyber tort] area are hesitant and incomplete, but two recent decisions from the federal courts of appeals point the way toward the development of this doctrine. The cases both involve third party liability . . . and are a step short of the product liability doctrines that would be inherent in software design claims.

21. Rustad & Koenig, *supra* note 20, at 116. The other subsets of cyber tort litigation identified by Professors Rustad and Koenig are "intentional torts, where the Internet is merely an instrumentality for civil wrongs, . . . and . . . the missing category of new cybertort duties and causes of action." *Id.* at 115–16.

22. 28 U.S.C. § 1604 (2012).

23. *Id.* §§ 1605(a)–(b). General exceptions to foreign-state immunity arise in cases of explicit or implicit waiver; commercial activity in or directly affecting the United States; property taken in violation of international law; rights to property acquired by succession or gift or rights to property located in the United States; personal injury, death, or damage or loss of property caused by a tortious act or omission that occurred in the United States; enforcement of an arbitration agreement made between a foreign state and a private party; and admiralty lawsuits to enforce a maritime lien based on commercial activity. *See id.*

24. Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852 (2016) (codified as amended at 28 U.S.C. § 1605B).

25. 28 U.S.C. § 1605(a).

exception.[26] However, in a recent decision addressing a cyber tort allegedly perpetrated by the Ethiopian government, the U.S. Court of Appeals for the D.C. Circuit introduced another hurdle to cyber tort victims, holding that the noncommercial tort exception does not apply when the intent to commit the tort is held by a party located outside of the United States.[27] Under this strict interpretation of the noncommercial tort exception, redress for victims of foreign-state-perpetrated cyber torts would be almost entirely foreclosed.[28]

This Note argues that the D.C. Circuit's extension of the "entire tort" doctrine to preclude jurisdiction over foreign states where the person holding the intent to commit the tort was abroad was misplaced. Instead, this Note proposes a test for courts to determine whether a cyber tort "occurred in the United States" modeled after current personal jurisdiction jurisprudence. The proposed test focuses on where the harm occurred rather than where the party harboring intent is located and is consistent with the original interpretation of the "entire tort" doctrine. In doing so, this Note resolves concerns posed by some scholars that the noncommercial tort exception is inapplicable to most cyber torts.[29] Part I discusses the history of foreign sovereign immunity and the current legal scheme in the United States. Part II introduces the current proposals for holding foreign states accountable for cyber torts, then examines the D.C. Circuit's holding in *Doe v. Federal Democratic Republic of Ethiopia* in more detail. Part III argues against the "entire tort" doctrine's application to determine the situs[30] of cyber torts and instead provides a modified jurisdictional test to determine whether a cyber tort occurred in the United States. This Note concludes by discussing why the proposed jurisdictional test is a better solution than the *Doe* court's approach.

---

26. *Id.* § 1605(a)(5).

27. 851 F.3d 7, 11–12 (D.C. Cir. 2017); *see also* 44B AM. JUR. 2D *International Law* § 159 (2017) (summarizing *Doe v. Federal Democratic Republic of Ethiopia* and other cases applying the "entire tort" doctrine).

28. This Note focuses on why the noncommercial tort exception includes intentional cyber torts committed by foreign sovereigns. Whether the proposed location test applies to negligence claims is beyond the scope of this Note.

29. *See infra* Part II.

30. "The location or position (of something) for legal purposes, as in *lex situs*, the law of the place where the thing in issue is situated." *Situs*, BLACK'S LAW DICTIONARY (10th ed. 2014).

I. THE U.S. APPROACH TO FOREIGN SOVEREIGN IMMUNITY

A. A Brief History of Foreign Sovereign Immunity

The concept of foreign sovereign immunity evolved from the prevailing view during the Middle Ages that all kings were of equal standing, and thus "one sovereign monarch could not be subject to the jurisdiction of another sovereign monarch."[31] The incorporation of this principle into U.S. law can be traced to Chief Justice John Marshall's opinion in *Schooner Exchange v. McFaddon*.[32] In concluding that foreign war ships were entitled to sovereign immunity, Chief Justice Marshall reasoned that the "perfect equality and absolute independence of sovereigns . . . have given rise to a class of cases in which every sovereign is understood to wave [sic] the exercise of a part of that complete exclusive territorial jurisdiction, which has been stated to be the attribute of every nation."[33] Subsequent cases extended the *Schooner* holding to other types of property,[34] cementing the absolute theory of sovereign immunity as the guiding principle in the United States.[35] The absolute theory of sovereign immunity held that "a sovereign cannot, without . . . consent, be made a respondent in the courts of another sovereign."[36] Under this theory of sovereign immunity, foreign states "enjoyed a high level of immunity and exceptions, if any, were not widely recognized."[37]

During the early-to-mid-twentieth century, countries began to move away from the absolute theory of foreign sovereign immunity and

---

31. JEFFREY L. DUNOFF ET AL., INTERNATIONAL LAW: NORMS, ACTORS, PROCESS: A PROBLEM-ORIENTED APPROACH 314–15 (4th ed. 2015).

32. 11 U.S. (7 Cranch) 116, 137, 145–46 (1812) (holding that it was "a principle of public law, that national ships of war, entering the port of a friendly power open for their reception, are to be considered as exempted by the consent of that power from its jurisdiction").

33. *Id.* at 137. This reasoning was based on the notions of international comity, in that

> [o]ne sovereign being in no respect amenable to another; and being bound by obligations of the highest character not to degrade the dignity of his nation, by placing himself or its sovereign rights within the jurisdiction of another, can be supposed to enter a foreign territory only under an express license, or in the confidence that the immunities belonging to his independent sovereign station, though not expressly stipulated, are reserved by implication, and will be extended to him.

Id.

34. *See, e.g.*, *Ex parte* Republic of Peru, 318 U.S. 578 (1943) (involving a claim brought against a foreign vessel for commercial activity); Berizzi Bros. Co. v. Pesaro, 271 U.S. 562 (1926) (involving a merchant vessel delivering damaged cargo).

35. Letter from Jack B. Tate, Acting Legal Adviser, U.S. Dep't of State, to Philip B. Perlman, Acting Attorney Gen., U.S. Dep't of Justice (May 19, 1952), *in* 26 DEP'T ST. BULL. 984, 984 (1952) [hereinafter Tate Letter].

36. *Id.*

37. Ingrid Wuerth, *Foreign Official Immunity Determinations in U.S. Courts: The Case Against the State Department*, 51 VA. J. INT'L L. 915, 925 (2011).

toward a more restrictive interpretation.[38] The restrictive theory of sovereign immunity recognizes "the immunity of the sovereign . . . with regard to sovereign or public acts (*jure imperii*) of a state, but not with respect to private acts (*jure gestionis*)."[39] Although U.S. courts in the eighteenth and nineteenth centuries deferred to the executive on some immunity questions,[40] they did not begin to more robustly defer immunity determinations to the executive until the mid-twentieth century.[41] In 1952, State Department acting legal adviser Jack Tate wrote a letter to the Attorney General ("Tate Letter"), stating that absolute immunity was no longer appropriate and that the State Department would follow the restrictive theory of sovereign immunity going forward.[42] Arguing that the restrictive theory would align the United States with the majority of other countries, Tate concluded that "the widespread and increasing practice on the part of governments of engaging in commercial activities makes necessary a practice which will enable persons doing business with them to have their rights determined in the courts."[43] Though this transition began shortly after the Tate Letter, the restrictive theory was not officially adopted until Congress codified it in 1976.[44]

B. Codifying the Restrictive View: The Foreign Sovereign Immunities Act of 1976

In 1976, the United States codified the restrictive approach to foreign sovereign immunity through the enactment of the FSIA.[45] In addition to providing statutory guidelines for determining foreign

38. DUNOFF ET AL., *supra* note 31, at 319 ("During the 1940s and 1950s, state practice moved away from the absolute theory. During this period, the State Department conducted a study of the relevant practices of other states and eventually reached the conclusion that immunity should not be granted in cases involving private, as contrasted with sovereign, acts.").

39. Tate Letter, *supra* note 35, at 984.

40. *See* Wuerth, *supra* note 37, at 924–25 ("Courts deferred to the executive on some questions, such as the existence of the government in question, but did not view themselves as bound by the executive's suggestion of immunity.").

41. *See Ex parte* Republic of Peru, 318 U.S. 578, 589 (1943) (holding that the State Department's recognition of Peru's claim of immunity "must be accepted by the courts as a conclusive determination by the political arm of the Government that the continued retention of the vessel interferes with the proper conduct of our foreign relations"); *see also* Republic of Mexico v. Hoffman, 324 U.S. 30, 35 (1945) (holding it was not for the judiciary to "deny an immunity which our government has seen fit to allow, or to allow an immunity on new grounds which the government has not seen fit to recognize").

42. *See* Tate Letter, *supra* note 35.

43. *Id.* at 985.

44. *See* Verlinden B.V. v. Cent. Bank of Nigeria, 461 U.S. 480, 487 (1983) ("On occasion, political considerations led to suggestions of immunity in cases where immunity would not have been available under the restrictive theory.").

45. 28 U.S.C. §§ 1602–1611 (2012).

immunity, the FSIA shifted the authority of determining whether a foreign state was immune from the executive branch to the judiciary.[46] Substantively, the FSIA broadly grants foreign states immunity from the jurisdiction of U.S. courts unless a statutory exception applies.[47] In addition to the foreign state itself, the statute extends immunity to "a political subdivision of a foreign state or an agency or instrumentality of a foreign state."[48] Although this definition of a foreign state broadens the reach of the FSIA tremendously, the statute's reach is not unlimited. The protections provided by the FSIA do not extend to individual government officials,[49] and it remains unclear whether the FSIA applies in criminal cases.[50]

---

46. *Id.* § 1602:

> The Congress finds that the determination by United States courts of the claims of foreign states to immunity from the jurisdiction of such courts would serve the interests of justice and would protect the rights of both foreign states and litigants in United States courts. . . . Claims of foreign states to immunity should henceforth be decided by courts of the United States and of the States in conformity with the principles set forth in this chapter.;

see also William F. Webster, Note, Amerada Hess Shipping Corp. v. Argentine Republic*: Denying Sovereign Immunity to Violators of International Law*, 39 HASTINGS L.J. 1109, 1109 (1988) ("Congress intended the Act to transfer from the executive branch to the judicial branch the decision whether to grant jurisdictional immunity to a sovereign defendant brought before American courts.").

47. 28 U.S.C. § 1604 ("Subject to existing international agreements to which the United States is a party at the time of enactment of this Act a foreign state shall be immune from the jurisdiction of the courts of the United States and of the States . . . ."); *see also* Saudi Arabia v. Nelson, 507 U.S. 349, 355 (1993) ("Under the Act, a foreign state is presumptively immune from the jurisdiction of United States courts; unless a specified exception applies, a federal court lacks subject-matter jurisdiction over a claim against a foreign state.").

48. 28 U.S.C. § 1603(a). In turn:

> An "agency or instrumentality of a foreign state" means an entity—(1) which is a separate legal person, corporate or otherwise, and (2) which is an organ of a foreign state or political subdivision thereof, or a majority of whose shares or other ownership interest is owned by a foreign state or political subdivision thereof, and (3) which is neither a citizen of a State of the United States as defined in section 1332 (c) and (e) of this title, nor created under the laws of any third country.

Id. § 1603(b).

49. *See* Samantar v. Yousuf, 560 U.S. 305, 308 (2010) (holding unanimously that the FSIA does not govern the immunity claims of individual foreign officials).

50. *Compare* Southway v. Cent. Bank of Nigeria, 198 F.3d 1210, 1215 (10th Cir. 1999) (extending jurisdiction under the FSIA in a civil RICO action even though RICO liability requires existence of indictable acts), *and* United States v. Noriega, 117 F.3d 1206, 1212 (11th Cir. 1997) ("[T]he FSIA addresses neither head-of-state immunity, nor foreign sovereign immunity in the criminal context . . . ."), *with* United States v. Hendron, 813 F. Supp. 973, 975 (E.D.N.Y. 1993) ("[T]he Act contains a panoply of provisions that are consistent only with an application to civil cases and not to criminal proceedings."), *and* Gould, Inc. v. Mitsui Mining & Smelting Co., 750 F. Supp. 838, 844 (N.D. Ohio 1990) (holding that neither the FSIA nor § 1330 confers jurisdiction over foreign states in criminal proceedings). Resolving the FSIA's applicability to criminal cases is beyond the scope of this Note.

Before delving into the specifics of the FSIA and whether its exceptions allow U.S. courts to hear cyber tort claims against foreign sovereigns, it is important to note that due process rights under the Fifth Amendment do not appear to extend to foreign sovereigns.[51] Though the U.S. Supreme Court has not directly addressed this issue, the Court has suggested as much.[52] Numerous courts of appeals have held that foreign states are not "persons" protected by the Fifth Amendment's Due Process Clause, and thus personal jurisdiction requirements do not apply.[53] Although some courts have extended this line of reasoning to some agencies and instrumentalities of foreign states,[54] an agency or instrumentality may be entitled to due process protections if a court determines that the agency or instrumentality has a different constitutional status than the foreign state that controls it.[55]

The determination of whether a foreign state is amenable to suit in U.S. courts largely hinges on whether cyber torts fall within one of the FSIA's exceptions—if the actions of the foreign state fall within one of the exceptions, the FSIA confers both subject matter and personal

---

51. For further discussion of whether foreign states and their agencies and instrumentalities have due process rights, see Ingrid Wuerth, Foreign Nations, Article III, and the Fifth Amendment Due Process Clause (Oct. 4, 2018) (unpublished manuscript) (on file with author).

52. *See* Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 619 (1992) (suggesting Fifth Amendment protections do not extend to foreign states); s*ee also* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 454 cmt. 9 (AM. LAW INST., Tentative Draft No. 3, 2017) ("[T]he Supreme Court has not resolved whether foreign states are 'persons' entitled to due-process protection.").

53. *See* Price v. Socialist People's Libyan Arab Jamahiriya, 294 F.3d 82, 96 (D.C. Cir. 2002) ("[Regarding statutes,] there is an often-expressed understanding that in common usage, the term 'person' does not include the sovereign, and statutes employing the word are ordinarily construed to exclude it." (internal quotation marks omitted) (quoting Will v. Mich. Dep't of State Police, 491 U.S. 58, 64 (1989))); *see also* Frontera Res. Azer. Corp. v. State Oil Co. of the Azer. Republic, 582 F.3d 393, 399 (2d Cir. 2009) ("If the States, as sovereigns that are part of the Union, cannot 'avail themselves of the fundamental safeguards of the Due Process Clause,' we do not see why foreign states, as sovereigns wholly outside the Union, should be in a more favored position." (citation omitted) (quoting *Price*, 294 F.3d at 97)). *Contra* Wuerth, *supra* note 51 (arguing that the Fifth Amendment's Due Process Clause protects foreign states).

54. *See, e.g.*, TMR Energy Ltd. v. State Prop. Fund of Ukr., 411 F.3d 296, 300–02 (D.C. Cir. 2005).

55. *Cf.* First Nat'l City Bank v. Banco Para el Comercio Exterior de Cuba (*Bancec*), 462 U.S. 611, 623–33 (1983) (establishing a rebuttable presumption that foreign-state-owned agencies carry a separate juridical status from the foreign government itself), *superseded on other grounds by* 28 U.S.C. § 1610(g)(1) (2012). Some courts of appeals have extended *Bancec*'s analysis of a foreign-state-owned agency's juridical status to the question whether a similar agency is entitled to due process protections. *See* Corporación Mexicana de Mantenimiento Integral v. Pemex-Exloración y Producción, 832 F.3d 92, 103 (2d Cir. 2016) ("Although *Bancec* arose in a different context, it is 'applicable when the question is whether the instrumentality should have due process rights to which the state is not entitled.' " (quoting *Frontera Res. Azer. Corp.*, 582 F.3d at 400)); *TMR Energy*, 411 F.3d at 301 ("We believe the [*Bancec*] analysis must govern whether the [state-owned agency] is a 'person' within the meaning of the due process clause . . . .").

jurisdiction over the foreign state.[56] The FSIA contains both general and specific exceptions to its broad grant of immunity.[57] The specific exceptions narrowly eliminate immunity for acts of terrorism and the material support thereof.[58] General exceptions to the FSIA include (1) waiver of immunity by the foreign state, (2) noncommercial tortious activity, (3) commercial activity, and (4) expropriations in violation of international law.[59]

It is unlikely that a cyber tort committed by a foreign state would fall under the exception for expropriations of property in violation of international law, as it is unclear whether electronic property can be taken.[60] Thus, unless a foreign state waives immunity, a cyber tort claim against a foreign state can only be brought in U.S. courts if either the commercial activity exception or the noncommercial tort exception is met. The Supreme Court has defined a foreign state's activity as commercial in nature only when it is "the *type* of action[ ] by which a private party engages in 'trade and traffic or commerce.' "[61] Because cyber torts are usually employed to steal information or impair the functionality of electronic systems, it is unlikely that cyber torts meet this definition of commercial activity.[62] However, the noncommercial tort exception is certainly relevant to the adjudication of cyber tort

56. *See* 28 U.S.C. §§ 1602–1611; *see also* Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 434 (1989) (holding that the FSIA is the "sole basis for obtaining jurisdiction over a foreign state"). Once an exception to the FSIA is met, § 1330 provides original jurisdiction to federal district courts. 28 U.S.C. § 1330(a) ("[D]istrict courts shall have original jurisdiction . . . of any nonjury civil action against a foreign state . . . [for in personam claims] with respect to which the foreign state is not entitled to immunity either under sections 1605–1607 of this title or under any applicable international agreement.").

57. 28 U.S.C. §§ 1605–1605B.

58. *Id.* § 1605A–1605B.

59. *Id.* § 1605(a).

60. *See* Paige C. Anderson, Note, *Cyber Attack Exception to the Foreign Sovereign Immunities Act*, 102 CORNELL L. REV. 1087, 1090–91 (2017) (acknowledging the lack of jurisprudence and scholarship on expropriations in the cyber context).

61. Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 614 (1992) (quoting *Commercial*, BLACK'S LAW DICTIONARY (6th ed. 1990)). Thus, whether a foreign state's actions are commercial depends on whether the government is acting as a "regulator of a market" or a "private player within it." *Id.*

62. Despite this distinction, the DNC's complaint against Russia appears to rely on both the noncommercial tort exception and the commercial activity exception. Complaint, *supra* note 7, ¶ 29. Some scholars, however, have expressed skepticism that the DNC has a plausible argument under the commercial activity exception. *See* Grayson Clary, *Under the Foreign Sovereign Immunities Act, Where 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 [https://perma.cc/ZEU5-BZCP] (noting that successfully invoking the commercial activity exception in the DNC's complaint would "require a difficult spatial analysis"); *see also* Ingrid Wuerth, *The DNC v. Russia: The Question of Foreign Sovereign Immunity*, LAWFARE (Apr. 22, 2018, 9:00 AM), https://www.lawfareblog.com/dnc-v-russia-question-foreign-sovereign-immunity [https://perma.cc/GDA3-XL46] (discussing the DNC's complaint in detail).

claims. Specifically, this exception allows claims for monetary damages against a foreign state (that are not covered by the commercial activity exception) to be brought in U.S. courts "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."[63] Part II of this Note explores the merits of applying the noncommercial tort exception to cyber torts and the current jurisprudence in this area.

II. DECODING THE RELATIONSHIP BETWEEN CYBER TORTS AND FOREIGN SOVEREIGN IMMUNITY

Acknowledging that technological advances have introduced novel forms of tortious conduct, scholars have proposed a variety of solutions to the difficulties of bringing cyber tort litigation against foreign states. The two most prominent suggestions are (1) interpreting the current noncommercial tort exception to include liability for cyber torts[64] and (2) passing a cyber tort–specific amendment to the FSIA that is modeled after the terrorism exception.[65] Section II.A explores whether cyber torts fall under the current language of the noncommercial tort exception. Section II.B discusses the relative merits of relying on a cyber tort–specific exception to provide redress to victims. Section II.C addresses reciprocity arguments against the inclusion of cyber torts within an exception to the FSIA. Finally, Section II.D takes an in-depth look at the D.C. Circuit's recent interpretation of the noncommercial tort exception in *Doe v. Federal Democratic Republic of Ethiopia*.

A. Interpreting the Noncommercial Tort Exception to Apply to Cyber Torts

The noncommercial tort exception to the FSIA[66] applies to "(1) a non-commercial tortious act or omission (2) committed by a state or its

63. 28 U.S.C. § 1605(a)(5). Claims based on "the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused," *id.* § 1605(a)(5)(A), and claims "arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights," *id.* § 1605(a)(5)(B), however, do not fall under the exception.

64. *See* Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, COLUM. HUM. RTS. L. REV., Spring 2015, at 227.

65. *See* Anderson, *supra* note 60.

66. 28 U.S.C. § 1605(a)(5):

agents that (3) causes personal injury or property damage [and] (4) occur[s] in the United States."[67] The first two elements rarely raise significant legal concerns and therefore do not warrant detailed analysis in this Note. Satisfying the latter two elements—the conduct causes "damage to or loss of property" and the conduct occurs in the United States—is more challenging in the cyber context.[68] This Section addresses each element in turn.

1. "Personal Injury or Death, or Damage to or Loss of Property"

The noncommercial tort exception's harm element is satisfied when either of its two prongs—"personal injury or death" or "damage to or loss of property"—are met. Though, at first glance, cyber torts do not typically cause "damage to or loss of property" in the traditional sense,[69] some cyber torts could impair system functionality[70] or otherwise damage physical property and thus satisfy this prong.[71] In fact, one such cyber tort was carried out against Iran. In what is largely believed to be a joint U.S.-Israeli project, Iranian nuclear power plants were infected with the Stuxnet virus, a malicious computer worm that "reportedly destroy[ed] roughly a fifth of Iran's nuclear centrifuges by

---

> A foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case . . . not otherwise encompassed in [the commercial activity exception], in which 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 . . . .

67. Gilmore, *supra* note 64, at 252–53 (footnote omitted).

68. Anderson, *supra* note 60, at 1094.

69. Of course, for a foreign state's conduct to implicate the noncommercial tort exception at all, the foreign state must violate domestic tort law. Although in many cases this is not an issue, some courts have held that some common law torts do not extend to the cyber context, even against domestic actors. *See, e.g.*, Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 359 (4th Cir. 2006) (discussing the possible nonexistence of a cyber trespass to chattels because the traditional tort requires physical contact with chattels); Inventory Locator Serv., LLC v. Partsbase, Inc., No. 02-2695 MA/V, 2005 WL 2179185, at *11–12 (W.D. Tenn. Sept. 6, 2005) (dismissing a trespass to chattels counterclaim because the electronic database that the plaintiff hacked was "not movable personal property"). The extent to which courts do or should recognize cyber torts is a topic beyond the scope of this Note.

70. *See* Intel Corp. v. Hamidi, 71 P.3d 296, 306 (Cal. 2003) (suggesting that limiting a server's functionality would qualify as damage to property). Additionally, software (the programming component of electronic devices) and hardware (the physical components) have a symbiotic relationship. Thus, even though cyber torts typically target software, the physical components of the machine can also suffer functional limitations or physical damage.

71. *See* Gilmore, *supra* note 64, at 265 ("[A]t common law, a violation of privacy is an injury to the psyche. And nothing in the FSIA contradicts that traditional understanding. Courts construing the FSIA should therefore follow the common law and treat electronic privacy violations as personal injuries.").

causing them to spin out of control."[72] It remains debatable whether cyber torts resulting in nontraditional harms—such as theft of bank details or other sensitive information—satisfy the "damage to or loss of property" requirement. Courts have employed various approaches to decide whether these types of injuries qualify as damage to or loss of property; they range from stringently requiring that a cyber tort limit the server's functioning[73] to more relaxed standards that demand only a showing of unauthorized use.[74]

Cyber torts are more likely to satisfy the harm element under its other prong: when a foreign state causes "personal injury." The FSIA does not define "personal injury," but *Black's Law Dictionary* defines "personal injury" as including "[*a*]*ny invasion* of a personal right, including mental suffering and false imprisonment."[75] Thus, cyber torts resulting in stolen bank information or confidential, proprietary technology would constitute an invasion of a personal right—the right to privacy—and satisfy the "personal injury" requirement. The Ninth Circuit applied this interpretation when it held that jurisdiction was proper over the plaintiff's privacy claim in *Alpha Therapeutic Corp. v. Nippon Hoso Kyokai*.[76] The claim alleged that a foreign-state-employed reporter secretly recorded an interview conducted at the plaintiff's home.[77] Similar to the injuries inflicted by most cyber torts, this secret interview recording would be unlikely to cause damage to or loss of property but nevertheless creates a personal injury.

2. "Occurring in the United States"

A more difficult hurdle for including cyber torts within the noncommercial tort exception is the "occurring in the United States" requirement.[78] This requirement hinges on what is considered to be the

---

72. Michael B. Kelly, *The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' than Previously Thought*, BUSINESS INSIDER (Nov. 20, 2013, 12:58 PM), http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11 [https://perma.cc/3VLX-3FYB].

73. *See Intel Corp.*, 71 P.3d at 306.

74. *See* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2226–32 (2004) (reviewing cases where courts allowed system owners to exclude unwanted uses if system owners provided strong signals that the uses were unwanted).

75. *Personal Injury*, BLACK'S LAW DICTIONARY (10th ed. 2014) (emphasis added). For further discussion of the merits of interpreting the personal injury or property damage requirement to include injuries caused by cyber torts, see Gilmore, *supra* note 64, at 262–65.

76. 199 F.3d 1078, 1088–89 (9th Cir. 1999) ("The district court determined that NHK implicitly conceded that Dr. McAuley's invasion of privacy claim fell within the tortious activity exception to the FSIA."), *order withdrawn on other grounds*, 237 F.3d 1007 (9th Cir. 2001).

77. *Id.* at 1083.

78. The Supreme Court appears to use the statutory language "occurring in the United States" and the language "committed in" interchangeably with regard to the noncommercial tort

situs of a cyber tort. Before the rapid advancement of technology and, with it, the proliferation of cyber torts, some courts viewed the requirement of "occurring in the United States" through the lens of the "entire tort" doctrine. This Section first traces the history and application of the doctrine and then argues against its application to cyber torts.

a. Determining the Situs of Traditional Torts Using the "Entire Tort" Doctrine

The "entire tort" doctrine can be traced to the D.C. Circuit's opinion in *Asociacion de Reclamantes v. United Mexican States*.[79] In *Asociacion de Reclamantes*, the plaintiffs represented the successors in interest of land grants from the King of Spain or Republic of Mexico that covered twelve million acres in modern-day Texas.[80] Though ownership of the land had been disputed since the Mexican-American War, a 1941 treaty released the United States from liability on any Mexican claim to the land grants at issue, with each country agreeing to satisfy the claims of its own nationals.[81] Over forty years later, the Mexican government had not paid a single claim to the successors in interest.[82] These successors then brought suit against the Mexican government in the United States and claimed that the U.S. courts had jurisdiction under the noncommercial tort exception to the FSIA.[83]

Although the initial tortious activity may have occurred on U.S. soil,[84] the crux of the plaintiffs' claims was Mexico's failure to provide compensation for the land grants.[85] As such, the court reasoned, "it [was] clear that the conduct complained of lack[ed] the required nexus with the United States."[86] Although the prior tortious activity was relevant to the plaintiffs' claim, the court concluded that it was

---

exception. *See* Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 439–41 (1989) (holding that damage to a ship located five thousand miles off the nearest U.S. coastline did not satisfy the "occurring in the United States" requirement of the noncommercial tort exception because the tort was not committed in U.S. "territory and waters, continental and insular," as defined by the FSIA).

79. 735 F.2d 1517 (D.C. Cir. 1984).

80. *Id.* at 1519.

81. *Id.*

82. *Id.*

83. *Id.* at 1524.

84. *Id.* ("It is not contended in the present case that any of Mexico's acts that could conceivably be regarded as having been committed on United States soil—the espousal, presentation and settlement of the claims—was in and of itself tortious.").

85. *Id.* at 1524–25.

86. *Id.* at 1524. The court further opined that "[a]lthough the statutory provision is susceptible of the interpretation that only the effect of the tortious action need occur here, where Congress intended such a result elsewhere in the FSIA it said so more explicitly." *Id.*

insufficient that only some acts causing the injury occurred on U.S. soil; instead, in order for the noncommercial tort exception to apply, *all* acts needed to occur in the United States.[87] The court concluded that it was "[declining] to convert [the noncommercial tort exception] into a broad exception for all alleged torts that bear some relationship to the United States."[88]

In *Jerez v. Republic of Cuba*, the D.C. Circuit expanded on this principle by holding that the "entire tort" doctrine is not satisfied when tortious conduct occurs abroad, even if the injury is experienced in the United States.[89] In this case, Jerez brought a tort claim against Cuba for the injuries he suffered while incarcerated in Cuba;[90] specifically, he experienced ongoing cirrhosis of his liver after Cuban officials allegedly injected him with Hepatitis C.[91] Although the injection of the virus occurred in Cuba,[92] Jerez claimed that the continued harms he experienced in the U.S. satisfied the "occurring in the United States" requirement.[93] The court rejected this argument, holding that the "entire tort" did not occur in the United States because the infliction of the injury occurred in Cuba, and consequently the action did not fall under the noncommercial tort exception to the FSIA.[94] However, the court left open the possibility that when a sovereign that intends to cause harm is located abroad but the injury occurs in the United States, a tort might satisfy the "occurring in the United States" requirement.[95]

---

87. *Id.* at 1525.

88. *Id.*

89. 775 F.3d 419, 424 (D.C. Cir. 2014) ("The law is clear that 'the entire tort'—including not only the injury but also the act precipitating that injury—must occur in the United States." (quoting *Asociacion de Reclamantes*, 735 F.2d at 1525)).

90. *Id.* at 421. Jerez was allegedly electrocuted, forced to live in inhospitable conditions, and purposefully injected with the Hepatitis C virus. *See id.* ("Readers familiar with *Against All Hope*, Armando Valladares's account of his incarceration by the same parties, will find much of Jerez's treatment similar to that inflicted on Valladares and depicted by him as having been extended to many of his fellow prisoners.").

91. *Id.* at 424.

92. *Id.* ("The problem for Jerez is that the defendants' alleged tort—purposefully injecting him with hepatitis C, otherwise subjecting him to conditions that caused hepatitis C, and failing to warn him of the virus—occurred in Cuba.").

93. *Id.*

94. *Id.* at 424–25. Jerez also argued that each replication of the Hepatitis C virus constituted a separate tort, and thus both the action and the injury occurred in the United States. The court similarly found this line of reasoning to be unpersuasive. *Id.* at 424.

95. *Id.* at 424. Jerez attempted to analogize his injury to the hypothetical situation of a foreign agent delivering an anthrax package or bomb to a recipient in the United States. The court distinguished Jerez's suit: "But here the defendants' infliction of injury on Jerez *occurred entirely in Cuba*, whereas the infliction of injury by the hypothetical anthrax package or bomb would *occur entirely in the United States*." *Id.* (emphasis added).

b. The Challenges of Determining the Situs of Cyber Torts

Applying the "entire tort" doctrine to determine where cyber torts occur is not as straightforward as with traditional tortious activity like that at issue in *Jerez* and *Asociacion de Reclamantes*.[96] In each case, it was easy to identify the physical locations where both the tortious action and injury took place. Cyber torts, however, are perpetrated through the use of cyberspace, the nature of which immediately complicates this analysis. In cyberspace, multiple people in different locations are able to concurrently access the same information. Similarly, dispersed data servers create the opportunity for a single action to impact numerous locations simultaneously. For example, a person located in Russia could hack a U.S. citizen's data, which is stored on a server in Canada. In this case, all three jurisdictions—Russia, the United States, and Canada—would be impacted at the same time by the same action. Conversely, a physical tort can only impact multiple locations in a sequential order.[97] The following example further illustrates the difficulties of determining where a cyber tort occurred.

Person *D*, a U.S. citizen, is targeted by the foreign government of Country *E* in response to Person *D* remotely assisting a human rights movement in Country *E*. Country *E* emails a software virus to Person *D*, whose computer is infected with the virus when he opens the email attachment. The software virus records all activity on the infected computer and sends the information to a server located in Country *E*. Person *D*, upon discovering the malicious software, intends to file suit against Country *E* for invasion of privacy in U.S. court.[98] However, in order to bring a proper suit against Country *E*, Person *D* must establish that U.S. courts have both subject matter and personal jurisdiction over Country *E* under the FSIA. To do so, Person *D* must show that the action occurred in the United States.

Given that data in cyberspace exists in multiple locations at the same time, how can a court reasonably determine the physical location of a cyber tort? The "entire tort" doctrine is ill suited to determine where a cyber tort occurred because the sovereign-tortfeasor most likely acted outside the United States and through an environment that does not have a single, discrete location. If all courts employed the "entire tort" doctrine to determine where a cyber tort occurs, a court would have

96. *Id.*; Asociacion de Reclamantes v. United Mexican States, 735 F.2d 1517 (D.C. Cir. 1984).

97. *See, e.g.*, *Jerez*, 775 F.3d 419 (declining applicability of noncommercial tort exception where the injury was first inflicted in Cuba and, after the victim travelled, its effects were later felt in the United States).

98. This hypothetical is loosely based on the facts of *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017).

jurisdiction to adjudicate a cyber tort only if the sovereign's agent is sitting in the United States when he inflicts harm, which is almost never the case. The D.C. Circuit's analysis of the fact pattern above, which this Note argues is erroneous, is examined *infra* Section II.D.

B. A Cyber Tort–Specific Exception to the FSIA Is Unnecessary

Some scholars have advocated for the passage of a cyber tort–specific exception modeled after the recently passed terrorism exception.[99] In her note, Paige Anderson argues that passage of such an amendment would "prevent[ ] claimants from having to rely on common-law precedent or ill-fitting statutes to assert their right to a remedy."[100] Although a newly passed exception would provide claimants with a private right of action that does not rely on the current exceptions to the FSIA, such an exception is not necessary to provide an avenue for relief and would significantly delay redress for victims.[101]

A cyber tort–specific amendment is unlikely to receive the same political support that was necessary to enact the FSIA's existing specific amendments. Nearly three thousand people perished in the September 11 attacks, which are widely accepted as the "worst and most audacious terror attack in American history."[102] In the aftermath of the attacks, Congress enacted a number of significant pieces of legislation, most of which garnered bipartisan support.[103] Although the effects of a cyber tort are devastating in their own right, it is simply hard to imagine that a cyber tort—even one affecting billions of users' data—could create

---

99. *See* Anderson, *supra* note 60. The terrorism exception is a specific exception to the FSIA that rescinds immunity from foreign states for "act[s] of torture, extrajudicial killing, aircraft sabotage, hostage taking, or the provision of material support or resources" provided that the foreign state "was designated as a state sponsor of terrorism at the time the act . . . occurred, or was so designated as a result of such act." 28 U.S.C. § 1605A (2012).

100. Anderson, *supra* note 60, at 1103.

101. *See supra* Section II.A (discussing the application of the noncommercial tort exception to cyber torts); *see also* Gilmore, *supra* note 64 (discussing the reasons the noncommercial tort exception applies to cyber torts).

102. Serge Schmemann, *U.S. ATTACKED; President Vows to Exact Punishment for 'Evil*,*'* N.Y. TIMES (Sept. 12, 2001), https://www.nytimes.com/2001/09/12/us/us-attacked-president-vows-to-exact-punishment-for-evil.html [https://perma.cc/HN5M-L6WL].

103. *See, e.g.*, USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (creating the National Security Division within the Department of Justice); Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (creating the Department of Homeland Security); Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001) (authorizing the creation of the Transportation Security Administration to replace the use of private security guards); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (amending various existing laws to expand the detection, prevention, and punishment of terrorism).

enough bipartisan political momentum and public support as those generated in response to the September 11 attacks.

Additionally, new FSIA exceptions must work their way through the slow legislative process, which would substantially delay a victim's ability to seek redress. The recently passed domestic-terrorism exception[104] to the FSIA is a perfect example of this; despite the bill's introduction in December 2009,[105] the bill was not passed until September 28, 2016.[106] Of course, the driving force behind the domestic-terrorism exception was to provide redress to victims of the September 11 attacks, which occurred fifteen years prior to the passage of the bill.[107] Although this time lapse is not necessarily dispositive of how other FSIA amendments would fare in Congress, the legislative process is often lengthy, and the sheer volume of bills proposed in Congress relative to those enacted is staggering, which gives plenty of reason to believe that an amendment is unlikely to provide immediate relief to victims.[108]

Thus, although a cyber tort–specific exception would address the jurisdictional questions discussed above, the uncertainty inherent in the legislative process and the likely lack of political motivation surrounding it renders this a less attractive option. Moreover, a more practical interpretation of the noncommercial tort exception renders any amendment unnecessary. And instead of waiting on the lengthy legislative process, victims would be able to rely on the current legal scheme to seek justice and recompense immediately. Additionally, using the current noncommercial tort exception to resolve cyber tort cases would allow courts to interpret various cyber tort cases and fact patterns under the noncommercial tort exception—thus enabling a future legislature to better craft a cyber tort–specific amendment that is appropriately tailored.

---

104. 28 U.S.C. § 1605B. In her note, Anderson proposes a cyber tort–specific amendment based on the narrower § 1605A terrorism exception, which allows claims to be brought against states designated as "state sponsor[s] of terrorism." Anderson, *supra* note 60; *see* 28 U.S.C. § 1605A. In contrast, the new § 1605B domestic-terrorism exception was enacted in direct response to the September 11 attacks and extends to states that have not been formally designated as state sponsors of terrorism. Section 1605B—the direct response to the September 11 attacks—was enacted more than fourteen years after the attacks.

105. Justice Against Sponsors of Terrorism Act, S. 2930, 111th Cong. (2009) (initial introduction).

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

107. *See* Patricia Zengerle, *Senate Passes Bill Allowing 9/11 Victims to Sue Saudi Arabia*, REUTERS (May 17, 2016, 11:38 AM), https://www.reuters.com/article/us-saudi-usa-congress/senate-passes-bill-allowing-9-11-victims-to-sue-saudi-arabia-idUSKCN0Y8239 [https://perma.cc/5HVT-EETQ].

108. *Statistics and Historical Comparison*, GOVTRACK, https://www.govtrack.us/congress/bills/statistics (last visited Dec. 17, 2018) [https://perma.cc/7QRQ-3HBQ] (showing the bill-enactment rate hovering around three percent in recent years).

C. Addressing Reciprocity Concerns

Any perceived broadening of the exceptions to foreign sovereign immunity raises reciprocity concerns. In vetoing JASTA, President Obama stressed that "reciprocity plays a substantial role in foreign relations, and numerous other countries already have laws that allow for the adjustment of a foreign state's immunities based on the treatment their governments receive in the courts of the other state."[109] He reasoned that enacting JASTA "could encourage foreign governments to act reciprocally and allow their domestic courts to exercise jurisdiction over the United States or U.S. officials . . . for allegedly causing injuries overseas via U.S. support to third parties."[110] Although interpreting the noncommercial tort exception as applying to cyber torts could similarly encourage reciprocal treatment of the United States, numerous other countries have already begun examining their laws to determine how to best address the novel threats posed by the digital age.[111]

The global acknowledgment of and fight against cyberthreats suggest that the United States will soon be accountable for state-sponsored cyber torts abroad, regardless of whether it similarly adapts its existing laws. Indeed, the German government suggested that foreign states would not be immune from suit for cyber torts, when it launched an investigation to determine whether there was sufficient evidence to bring suit in German court against the United States for the alleged hacking of Chancellor Merkel's cellular phone.[112] Interpreting the noncommercial tort exception to include cyber torts could deter foreign states from engaging in illicit cyberactivity, as the foreign states would be on notice that they could not use a loophole in the FSIA to escape liability. This deterrent effect would only strengthen

---

109. Message to the Senate Returning Without Approval the Justice Against Sponsors of Terrorism Act, 2016 DAILY COMP. PRES. DOC. 628 (Sept. 23, 2016).

110. *Id.*

111. *See* ERIK BRATTBERG & TIM MAURER, CARNEGIE ENDOWMENT FOR INT'L PEACE, RUSSIAN ELECTION INTERFERENCE: EUROPE'S COUNTER TO FAKE NEWS AND CYBER ATTACKS (2018), https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf [https://perma.cc/58PV-BQ7B] (discussing various countries' approaches to counter and address election interference and hacking); *see also* Kristin Carlberg, Suing a State for Cross-Border Cyber Torts? Overcoming the Immunity of the Hacking State (Spring 2017) (unpublished magister thesis, Örebro Universitet), http://www.diva-portal.se/smash/get/diva2:1147530/FULLTEXT02.pdf [https://perma.cc/256Q-SM3D] (arguing in support of extending tortious-activity exceptions to certain kinds of cyberthreats).

112. *See Snowden NSA: Germany Drops Merkel Phone-Tapping Probe*, BBC NEWS (June 12, 2015), https://www.bbc.com/news/world-europe-33106044 [https://perma.cc/6WG6-P8BK]. German prosecutors dropped the investigation due to insufficient evidence, not because there were jurisdictional barriers to redress. *See id.*

if additional countries adopted similar measures to hold foreign states accountable for cyber torts. Cyberspace provides unprecedented access to individuals and their personal information and property; given this, all countries should welcome accountability measures that deter other foreign states from using cyberspace for nefarious purposes.

D. The Latest Chapter: The D.C. Circuit's Decision in Doe v. Federal Democratic Republic of Ethiopia

In 2017, the D.C. Circuit heard arguments in an appeal brought by one Kidane for cyber torts allegedly committed by the Ethiopian government.[113] Kidane, a former Ethiopian citizen, obtained asylum in the United States amid political strife in Ethiopia in the early 1990s.[114] While residing in the United States, Kidane provided technical and administrative support to the Ethiopian diaspora, some members of which participated in protests of political corruption and human-rights abuses in Ethiopia.[115] In late 2012 or early 2013, Kidane opened an email attachment sent to him by an acquaintance.[116] His computer was then infected with FinSpy, a remote-monitoring program.[117] After the program was installed, it allegedly recorded "some, if not all, of the activities undertaken by users of the computer."[118] This information was then communicated to a server located in Ethiopia.[119]

Alleging that the Ethiopian government was responsible for the installation of FinSpy on his computer, Kidane filed suit in U.S. federal district court, seeking redress under the Wiretap Act and the Maryland common law tort of intrusion upon seclusion.[120] At issue before the D.C. Circuit was whether the district court properly dismissed the case for lack of subject matter jurisdiction over Ethiopia because the FSIA's noncommercial tort exception was not satisfied.[121] In affirming, the D.C. Circuit relied on the application of the "entire tort" doctrine discussed

113. Doe v. Federal Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017). Although the named plaintiff-appellant in the case is John Doe, he is referred to in the proceedings by the pseudonym "Kidane." *Id.* at 8.

114. *See id.* at 8; Motion for Leave to Proceed in Pseudonym at 2, Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp. 3d 6 (D.D.C. 2016) (No. 1:14-cv-00372-RDM).

115. *Doe*, 851 F.3d at 8; Motion for Leave to Proceed in Pseudonym, *supra* note 114, at 2.

116. *Doe*, 851 F.3d at 8.

117. *Id.* FinSpy is a remote monitoring program sold exclusively to government agencies that allows them to "monitor[ ] and gather[ ] information from electronic devices, including computers and mobile phones, without the knowledge of the device's user." *Id.* at 8–9.

118. *Id.* at 9.

119. *Id.*

120. *Id.*

121. *Id.*

above.[122] To bolster his jurisdictional argument, Kidane identified several instances where the noncommercial tort exception permitted jurisdiction over foreign states even though the intent to commit tortious activity was held by a party located abroad.[123] Nevertheless, the D.C. Circuit held that "Ethiopia's digital espionage is of a different character. 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."[124]

Kidane then turned to the legislative intent of the noncommercial tort exception, arguing that the lack of limiting language in the statute suggests that the drafters did not intend to require that all aspects of the tort occur in the United States.[125] Congress rejected the European Convention on State Immunity's approach, which requires that tort was committed in the foreign state and that "the author of the injury or damage was present in that territory at the time."[126] Kidane additionally pointed to the Supreme Court's interpretation of the "carried on in the United States" requirement of the commercial activity exception to the FSIA.[127] Rejecting the comparison to the commercial activity exception, the D.C. Circuit reasoned that, "unlike the commercial activity exception, the noncommercial-tort exception does not ask where the 'gravamen' occurred; instead, it asks where the '*entire* tort' occurred."[128] Viewing Ethiopia's alleged involvement as similar to the Cuban government injecting Jerez with Hepatitis C during his incarceration, the D.C. Circuit ultimately held that the noncommercial tort exception did not apply because the "entire tort" did not occur in the United States.[129] As previously discussed, this line of reasoning oversimplifies the locational status of cyber torts. In doing so, the D.C. Circuit effectively foreclosed any possibility for victims of cyber torts to hold foreign states responsible.

---

122. *Id.* at 9–10; *see supra* Section II.A.2.a.

123. This argument and the cases relied on by Kidane are further discussed *infra* Section III.A.

124. *Doe*, 851 F.3d at 11.

125. *Id.*

126. *Id.* (internal quotation marks omitted) (quoting European Convention on State Immunity art. 11, May 16, 1972, E.T.S. No. 74, *reprinted in Jurisdiction of U.S. Courts in Suits Against Foreign States: Hearing on H.R. 11,315 Before the Subcomm. on Admin. Law & Governmental Relations of the H. Comm. on the Judiciary*, 94th Cong. 39 (1976)).

127. *Id.*

128. *Id.* (citation omitted) (first quoting OBB Personenverkehr AG v. Sachs, 136 S. Ct. 390, 396 (2015); then quoting Asociacion de Reclamantes v. United Mexican States, 735 F.2d 1517, 1525 (D.C. Cir. 1984)). Of note, this interpretation of the FSIA relies not on the text of the statute but on the interpretation of the exception in prior cases. *See supra* Section II.A.2.a.

129. *Doe*, 851 F.3d at 11–12.

III. PURSUING JUSTICE: PROVIDING CYBER TORT VICTIMS AN AVENUE FOR REDRESS

As discussed above, the D.C. Circuit's approach in *Doe* effectively gives foreign states carte blanche to perpetrate cyber torts against individuals and entities in the United States with little fear of suffering any legal repercussions. Section III.A argues that courts should not apply the "entire tort" doctrine to cyber torts as the D.C. Circuit did in *Doe*. As an alternative to the "entire tort" approach, Section III.B proposes a location test modeled after the personal jurisdiction "effects" test established in *Calder v. Jones*.[130] The proposed test allows courts to distinguish between cyber torts that have a direct relationship with the United States—based upon the foreign state's connection to the United States—and those with a more tenuous relationship based solely upon the victim's relationship to the United States. Although the jurisdictional test in *Calder*—and the refined test later applied in *Walden v. Fiore*[131]—hinged on whether the defendant's actions or the effects therefrom formed a relationship with a particular state,[132] this principle can be expanded to whether a defendant's actions are sufficient to establish a relationship with the United States as a whole, as is required by the noncommercial tort exception to the FSIA.

A. The D.C. Circuit's Approach Should Be Abandoned

If widely accepted by other circuits, the reasoning employed by the D.C. Circuit in *Doe* would make it practically impossible to bring cyber tort claims against foreign states, regardless of how egregious the offense.[133] Setting aside the lack of redress, there are a number of additional reasons why courts should not adopt the *Doe* court's interpretation of the "occurring in the United States" requirement. As a preliminary matter, the "entire tort" language relied on by the *Doe* court does not appear in the FSIA.[134] Rather, the "entire tort" language comes from lower-court jurisprudence that was popularized following the D.C. Circuit's decision in *Jerez*.[135] Additionally, the Supreme Court

130. 465 U.S. 783 (1984).

131. 571 U.S. 277 (2014).

132. *See* 465 U.S. at 789.

133. The nature of cyber torts makes it unlikely that the action taken to commit a cyber tort and the subsequent harm experienced will occur in the same place.

134. *See* 28 U.S.C. § 1605(a)(5) (2012). The "entire tort" interpretation of the "occurring in the United States" requirement also seems inconsistent with the commercial activity exception to the FSIA, which contains no comparable restriction. *See* 28 U.S.C. § 1605(a)(2).

135. *See supra* Section II.A.2.a (discussing the history of the "entire tort" doctrine).

has not adopted the "entire tort" doctrine,[136] and it has not been universally adopted across circuits with regard to traditional tort claims.[137]

Moreover, interpreting the noncommercial tort exception in this way is inconsistent with the commercial activity exception, as the commercial activity exception contains no comparable restriction. Though some may argue that *Republic of Argentina v. Weltover, Inc.*—the Supreme Court's landmark case interpreting the commercial activity exception—should be read to require that all elements of a plaintiff's claim occur in the United States, this is not what the opinion actually held.[138] Rather, the Court in *Weltover* rejected the requirements of foreseeability and substantiality required by some states' long-arm statutes[139] and instead focused the inquiry on whether the effect of the activity itself was direct.[140]

Such an interpretation also runs counter to the overarching goal of the noncommercial tort exception.[141] The noncommercial tort exception prevents foreign officials from escaping liability for noncommercial torts and provides an avenue for recourse to victims.[142] Though dramatic technological advances have altered the scope and substance of sovereign relationships since the FSIA's passage in 1976,

---

136. *See* Republic of Argentina v. Weltover, Inc., 504 U.S. 607 (1992); Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428 (1989).

137. The First, Second, Fifth, Sixth, Ninth, Tenth, and D.C. Circuits have all adopted or indicated in dicta that they approve of some iteration of the "entire tort" doctrine. *See, e.g.*, O'Neill v. Saudi Joint Relief Comm. (*In re* Terrorist Attacks on September 11, 2001), 714 F.3d 109, 115–16 (2d Cir. 2013); O'Bryan v. Holy See, 556 F.3d 361, 382 (6th Cir. 2009). Courts within the Ninth and D.C. Circuits, however, have held that the noncommercial tort exception applies to countries whose liability-inducing actions occurred abroad. *See* Liu v. Republic of China, 892 F.2d 1419, 1431 (9th Cir. 1989); Letelier v. Republic of Chile, 488 F. Supp. 665, 673 (D.D.C. 1980).

138. *See* 504 U.S. 607.

139. *Id.* at 618 ("[W]e reject the suggestion that § 1605(a)(2) contains any unexpressed requirement of 'substantiality' or 'foreseeability.' "); *see also* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 454 cmt. 8 (AM. LAW INST., Tentative Draft No. 3, 2017) ("An effect is not direct if it is a remote or attenuated consequence of the act. . . . Personal injury sustained in the United States as a result of a foreign sovereign's tortious conduct elsewhere can constitute a direct effect.").

140. *See Weltover*, 504 U.S. at 618 ("[A]n effect is 'direct' if it follows 'as an immediate consequence of the defendant's . . . activity.' " (omission in original) (quoting Weltover, Inc. v. Republic of Argentina, 941 F.2d 145, 152 (2d Cir. 1991))).

141. *See* S. REP. NO. 94-1310, at 11–12 (1976); H.R. REP. NO. 94-1487, at 14 (1976) (acknowledging "a wide acceptance . . . that the sovereign immunity of foreign states should be 'restricted' to cases involving acts . . . which are sovereign or governmental in nature, as opposed to acts which are . . . commercial in nature").

142. S. REP. NO. 94-1310, at 20–21; H.R. REP. NO. 94-1487, at 14, 20–21; *see also* Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 439–40 (1989) ("Congress' primary purpose in enacting § 1605(a)(5) was to eliminate a foreign state's immunity for traffic accidents and other torts committed in the United States, for which liability is imposed under domestic tort law.").

the reasoning behind the noncommercial tort exception remains relevant. In the context of cyber torts, the *Doe* court's interpretation of "occurring in the United States" would do precisely what the legislature sought to prevent—provide foreign states carte blanche to escape liability for private actions that harm individuals in the United States.

Indeed, holding foreign states accountable for tortious conduct that did not entirely occur within the United States is not novel. For example, in *Liu v. Republic of China*, the Ninth Circuit held that the noncommercial tort exception applied when two gunmen, acting on the orders of a Taiwanese admiral, assassinated a man in California, even though the actions conferring liability on China occurred abroad.[143] Similarly, in *Letelier v. Republic of Chile*, the U.S. District Court for the District of Columbia ruled that jurisdiction was proper under the noncommercial tort exception when Chilean government agents, operating under Chilean government instructions, constructed, planted, and detonated a car bomb in Washington, D.C.[144] In *Doe*, the court reasoned that these cases were distinguishable from Ethiopia's conduct because "[b]oth involved actions 'occurring in the United States' that were—without reference to any action undertaken abroad—tortious."[145] However, it was not alleged in *Liu* or *Letelier*—nor could it be—that the actions giving rise to the claims were committed directly by the foreign states on U.S. soil; rather, in both cases, the individuals who ultimately carried out the torts were acting under the direction of officials sitting in the foreign state.[146] Although the tortious activity alleged in these cases occurred in the United States, the actions for which the courts held the foreign states liable occurred abroad.[147]

Finally, the "entire tort" doctrine's focus on territory and location does not make sense in the context of cyber torts. Cyber torts target electronically stored data, and although the machines that access this data are tangible objects, the data itself lacks a physical form. In *Jerez*, the court differentiated between the site of the initial injury and

143. 892 F.2d 1419, 1422, 1431 (9th Cir. 1989).

144. 488 F. Supp. 665, 665–66, 673 (D.D.C. 1980).

145. Doe v. Federal Democratic Republic of Ethiopia, 851 F.3d 7, 11 (D.C. Cir. 2017).

146. *See Liu*, 892 F.2d at 1421 ("Two gunmen acting on orders of Admiral Wong Hsi-ling (Wong), Director of the Defense Intelligence Bureau (DIB) of the Republic of China (ROC), shot and killed Henry Liu in Daly City, California."); *Letelier*, 488 F. Supp. at 665–66 ("[The crime was committed by individuals] acting in concert and purportedly at the direction and with the aid of defendants Republic of Chile, its intelligence organ the Centro Nacional de Intelligencia (CNI) (formerly Direccion de Intelligencia Nacional, a/k/a DINA), and supposed CNI-DINA agents and officers . . . .").

147. *See Liu*, 892 F.2d at 1422 (describing directions given in China by Admiral Wong Hsi-ling); *Letelier*, 488 F. Supp. at 665–66 (describing directions and aid provided by government officials in Chile).

the continued effects of that injury experienced in the United States.[148] The court held that the replication of the Hepatitis C virus in Jerez did not constitute a separate tort, and Cuba's conduct thus did not meet the noncommercial tort exception because the original injection of the virus occurred in Cuba.[149] This is distinguishable from the cyber tort at issue in *Doe* because the harmful action in *Jerez* was inflicted on a tangible being in a particular location, while the action in *Doe* was directed at data that exists in multiple locations simultaneously. The victims for whom this Note seeks to protect do not travel to the United States after a tort is committed; rather, the victims are located in the United States at the time the tort occurs.

B. Relying on Established Jurisprudence to Determine Location

The rejection of the "entire tort" approach employed in *Doe* requires an alternative approach to determine where a cyber tort occurs. Should the location ascribed to a tort focus on where the precipitating conduct occurred, where it had an effect, or perhaps some intermediate location along the cyber tort's transmission path (such as a satellite or server)? This Note proposes an alternative interpretation of the "occurring in the United States" requirement of the FSIA's noncommercial tort exception to answer these questions. Specifically, courts should determine whether the foreign state (1) acted intentionally, (2) expressly aimed the action at a victim in the United States, and (3) knew or should have known that the brunt of the injury would be felt in the United States.[150] An objective knowledge standard for the third prong of this test allows courts to consider the resources and intelligence uniquely available to foreign states. If the court determines that the foreign state's express actions satisfy each prong of the analysis, the cyber tort in question "occurred in the United States" for the purposes of the FSIA's noncommercial tort exception.

This effects test is similar to the one employed by the Supreme Court in *Calder v. Jones*[151] and *Walden v. Fiore*.[152] In *Calder*, Shirley Jones, an actress who lived and worked in California, brought a libel

148. Jerez v. Republic of Cuba, 775 F.3d 419, 424 (D.C. Cir. 2014) ("[T]he continued replication of hepatitis C and Jerez's cirrhosis of the liver describe an ongoing *injury* that he suffers in the United States *as a result* of the defendants' acts in Cuba." (emphasis added)).

149. *See id.* ("The law is clear that 'the entire tort'—including not only the injury but also the act precipitating the injury—must occur in the United States.").

150. Similar to the approach used in *Calder v. Jones*, the inquiry into whether the brunt of the injury would be felt in the United States is fact-based and asks whether the ultimate harm was intended to be felt in the United States. *See* 465 U.S. 783, 789 (1984).

151. *See id.*

152. *See* 571 U.S. 277 (2014).

suit in California state court over an article published in the *National Enquirer*.[153] The author and the editor of the article, both of whom resided in Florida, argued that California state courts lacked personal jurisdiction over them because neither had physical contacts with California.[154] Unpersuaded that physical presence in the forum state was required to confer jurisdiction, the court held that personal jurisdiction in California was proper over the Florida defendants because the defendants' actions were (1) intentional, (2) "expressly aimed" at the forum state, and (3) committed knowing that the "brunt of that injury would be felt" in the forum state.[155]

The Court later refined this test in *Walden v. Fiore*, where it distinguished between a defendant's *mere knowledge* that harm would ultimately be felt in a specific location and a defendant's express aim of the action at that location.[156] In *Walden*, a group of drug enforcement officers seized $97,000 at Atlanta Hartfield-Jackson International Airport from two passengers travelling from San Juan to Las Vegas.[157] When one of the agents refused to return the seized money, the passengers brought suit against him in the U.S. District Court for the District of Nevada.[158] The Supreme Court held that the district court lacked personal jurisdiction.[159] In doing so, the Court reasoned that "[f]or a State to exercise jurisdiction consistent with due process, the defendant's suit-related conduct must create a *substantial connection* with the forum State."[160] The Court further explained that "however significant the plaintiff's contacts with the forum may be, those contacts cannot be 'decisive in determining whether the defendant's due process rights are violated.' "[161] Lower courts have held that this inquiry does not change when determining whether cyberactivity confers jurisdiction.[162]

---

153. 465 U.S. at 784–85.

154. *Id.*

155. *Id.* at 789–90; *see also* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 478–79 (1985) (holding that personal jurisdiction was proper where the defendant deliberately reached out to a forum citizen).

156. 571 U.S. at 290.

157. *Id.* at 279–80.

158. *Id.* at 281.

159. *Id.* at 282.

160. *Id.* at 284 (emphasis added).

161. *Id.* at 285 (quoting Rush v. Savchuk, 444 U.S. 320, 332 (1980)).

162. *See* Christie v. Nat'l Inst. for Newman Studies, 258 F. Supp. 3d 494, 500 (D.N.J. 2017) ("[W]hether tortious conduct is committed via the Internet or in more traditional means, does not change the inquiry of the location where Defendants purposefully aimed their alleged cyberactivity."); *see also* Revell v. Lidov, 317 F.3d 467, 473–75 (5th Cir. 2002); ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 714–15 (4th Cir. 2002); River City Media, LLC v.

The underlying concern that motivated the Court in *Walden*—limiting personal jurisdiction over defendants with too attenuated a relationship with the forum state[163]—parallels concerns raised by the court in *Jerez*: that the relationship between Cuba's actions and the United States was insufficient to satisfy the "occurring in the United States" requirement under the FSIA.[164] Taking these concerns into account, the location test proposed by this Note requires courts to determine whether the foreign state's actions satisfy the "occurring in the United States" requirement based on the *express actions* of the foreign state and whether those actions created a substantial connection with the United States. The express-action requirement adopts the reasoning of the *Walden* court and draws a sharp distinction between the relationship with the United States initiated by the foreign state and any tangential relationship that results from the victim's ties. This proposed test not only falls within the parameters of domestic personal jurisdiction jurisprudence; it also allows courts to adhere to the legislative reasoning behind the adoption of the noncommercial tort exception—holding foreign sovereigns liable for torts committed in violation of U.S. law.[165]

Although the Supreme Court has implied that due process rights and their corresponding personal jurisdiction limitations do not apply to foreign states,[166] the Court's personal jurisdiction jurisprudence provides an apt framework for a location test under the noncommercial tort exception.[167] Additionally, some lower courts have recognized that some agencies and instrumentalities of foreign states are entitled to due process protections.[168] As a result, these lower courts already engage in

---

Kromtech All. Corp., No. 2:17-cv-00105-SAB, 2017 U.S. Dist. LEXIS 137938, at *16–17 (E.D. Wash. 2017); Verizon Online Servs., Inc. v. Ralsky, 203 F. Supp. 2d 601, 612–17 (E.D. Va. 2002).

163. See *supra* Section I.B for a discussion of why due process protections likely do not extend to foreign states or some of their agencies and instrumentalities.

164. *See* Jerez v. Republic of Cuba, 775 F.3d 419, 424 (D.C. Cir. 2014) ("The problem for Jerez is that the defendants' alleged tort . . . occurred in Cuba.").

165. S. REP. NO. 94-1310, at 20–21 (1976); H.R. REP. NO. 94-1487, at 20–21 (1976).

166. *See supra* Section I.B.

167. Although the Court's personal jurisdiction jurisprudence is viewed by some scholars as incoherent, *see* Patrick J. Borchers, *Extending Federal Rule of Civil Procedure 4(k)(2): A Way to (Partially) Clean Up the Personal Jurisdiction Mess*, 67 AM. U. L. REV. 413 (2017), the Court's decision in *Walden* has been viewed by some as refining the personal jurisdiction test laid out in *Calder*, *see* Cassandra Burke Robertson & Charles W. "Rocky" Rhodes, *The Business of Personal Jurisdiction*, 67 CASE W. RES. L. REV. 775, 781 (2017). By adopting components of one portion of personal jurisdiction jurisprudence, this Note's solution avoids engaging with the incoherence expressed by scholars about personal jurisdiction jurisprudence overall. Moreover, the legislative history of the FSIA seems to suggest that Congress expected personal jurisdiction limitations to apply in some cases. *See infra* note 179 and accompanying text.

168. *See generally Bancec*, 462 U.S. 611, 623–33 (1983) (establishing a rebuttable presumption that foreign-state-owned agencies carry a separate juridical status than the foreign government itself). For a foreign state's agency or instrumentality to be entitled to due process protections, the

a *Bancec* constitutional analysis in FSIA cases brought against agencies and instrumentalities to determine whether due process protections apply.[169] This Note's proposed location test applies personal jurisdiction principles—regardless of whether they are constitutionally required—to all defendants under the FSIA and thus effectively applies due process limitations on personal jurisdiction to all defendants sued under the noncommercial tort exception. As a result, courts need not engage in a separate *Bancec* constitutional analysis to determine whether agencies and instrumentalities are entitled to due process protections; a location test that already incorporates these constitutional protections renders that determination unnecessary.

The following two hypothetical scenarios illustrate how the proposed location test would function.

1. An In-Scope Scenario

Country *A*, incensed over Company *B*'s recent film that made Country *A*'s leader look foolish, hacks Company *B*, a U.S. corporation headquartered in California. The hack deletes key data relating to the aforementioned film and steals privileged information about Company *B*'s proprietary technology, staff, and confidential communications. In hopes of further frustrating Company *B*'s ability to profit from the film, Country *A* releases sensitive information about Company *B*'s hiring practices and salary discrepancies, which was gleaned from the data stolen during the hack. As a result of Country *A*'s actions, Company *B*'s revenue severely decreases.[170] Under the approach proposed above, the "occurring in the United States" requirement would be satisfied because Country *A* (1) acted intentionally, (2) expressly aimed its conduct at Company *B*, a U.S. corporation, and (3) knew or should have known that the brunt of the injury—Company *B*'s decreased revenue and the privacy violations—would be felt by Company *B* in the United States.

The DNC's complaint against Russia, mentioned earlier, would similarly satisfy the "occurring in the United States" requirement.[171] In its complaint, the DNC alleged that the Russian government launched numerous cyberattacks on DNC servers located in Virginia and

agency or instrumentality must have a different constitutional status than the foreign state itself. *See* Corporación Mexicana de Mantenimiento Integral v. Pemex-Exloración y Producción, 832 F.3d 92, 103 (2d Cir. 2016); GSS Grp. Ltd. v. Nat'l Port Auth., 680 F.3d 805, 814–15 (D.C. Cir. 2012); TMR Energy Ltd. v. State Prop. Fund of Ukr., 411 F.3d 296, 301 (D.C. Cir. 2005).

169. *See TMR Energy*, 411 F.3d at 301.

170. This hypothetical is loosely based on the alleged hack perpetrated against Sony by North Korea. *See* Sanger & Perlroth, *supra* note 16.

171. *See supra* note 7 and accompanying text.

Washington, D.C., during the 2016 presidential election.[172] The attacks were purportedly carried out by Russian GRU[173] agents acting pursuant to orders from "high-ranking Russian officials."[174] Assuming these allegations are true—and despite the assertion from the Russia government that jurisdiction would "violate international law"[175]—the court would determine that the hack occurred in the United States because (1) the Russian GRU agents acted intentionally when they (2) targeted DNC servers located in the United States, and (3) Russia knew or should have known that the brunt of the injury would be felt in the United States, as the identified purpose of the hacks was to undermine Hillary Clinton's presidential campaign.[176] Therefore, the proposed location test would conclude that the alleged hacks occurred in the United States for purposes of the noncommercial tort exception.

2. An Out-of-Scope Scenario

Person *X*, a U.S. citizen known for his investigative-journalism pieces that expose foreign leaders' less-than-savory behavior, is travelling in Country *Y*. While in Country *Y*, Person *X*'s computer is purposely infected with malware by Country *Y*'s government. The malware provides Country *Y* with access to Person *X*'s banking information as well as other sensitive data.[177] Country *Y* uses this information to blackmail Person *X* into turning over the information he had relating to Country *Y*'s government officers. Upon returning to the United States, Person *X* files suit in federal district court, claiming jurisdiction under the noncommercial tort exception to the FSIA for the

172. *See* Complaint, *supra* note 7, ¶¶ 66, 77–78, 81; *see also* Jury Demand & Amended Complaint, *supra* note 7, ¶¶ 81–84.

173. The GRU is the English equivalent of the Russian acronym ГРУ and is commonly used to refer to the Russian Main Intelligence Directorate of the armed forces. *See* Alex Seitz-Wald, *What Is the GRU? Mueller Indicted the Spy Agency's Operatives*, NBC NEWS (July 13, 2018, 2:15 PM), https://www.nbcnews.com/politics/white-house/what-gru-mueller-indicted-spy-agency-s-operatives-n891291 [https://perma.cc/55TE-KA35].

174. *See* Complaint, *supra* note 7, ¶ 77; *see also* Jury Demand & Amended Complaint, *supra* note 7, ¶¶ 81–84.

175. Letter from Anatoly I. Antonov, Ambassador of the Russian Fed'n to the U.S., to Hon. John G. Koeltl, U.S. Dist. Judge, Democratic Nat'l Comm. v. Russian Federation, No. 1:18-cv-03501-JGK (S.D.N.Y. Nov. 9, 2018) ("I have the honor to also inform the Honorable Court that exercise of jurisdiction over the pending case by U.S. courts with respect to the Russian Federation is a violation of the international law . . . arising from the principle of the sovereign equality of states."). For a detailed discussion of the DNC's complaint and the Russian Federation's assertion of immunity in this case, see Ingrid Wuerth, *Russia Asserts Immunity in the DNC Case*, LAWFARE (Nov. 16, 2018, 10:14 AM), https://www.lawfareblog.com/russia-asserts-immunity-dnc-case [https://perma.cc/UQ84-3C5Q].

176. *See* Complaint, *supra* note 7, ¶¶ 55, 57, 61.

177. This hypothetical is loosely based on the facts of *Jerez v. Republic of Cuba*, 775 F.3d 419, 421 (D.C. Cir. 2014), except it uses a cyber tort instead of the physical harm that Jerez suffered.

resulting harms he experienced upon returning to the United States. Under the proposed test, this claim would fail the "occurring in the United States" requirement. Although the actions of Country *Y* were intentional, they do not satisfy the second prong of the test. The only connections between the United States and the actions of Country *Y* are the nationality of Person *X* and the assumption that Person *X* would return to the United States in the future. Thus, the connection between the United States and the alleged actions of Country *Y* relies entirely on Person *X*'s relationship with the United States. This connection, similar to that in *Walden* between the defendants and Nevada, is too attenuated to confer jurisdiction.[178]

3. Summarizing the Proposed Location Test

As illustrated by these examples, the adoption of the proposed test would align U.S. courts' treatment of cyber torts perpetrated by foreign states with the courts' jurisprudence of traditional torts. Therefore, in instances where a cyber tort was directed at an individual or corporation in the United States, such as in *Doe* or Scenario 1, the FSIA's noncommercial tort exception would apply and thus confer jurisdiction to U.S. courts. Conversely, if the alleged cyber tort was not directed at someone in the United States, as discussed in Scenario 2, the action would not satisfy the proposed location test and would not fall under the noncommercial tort exception. Interpreting the location requirement in this way holds foreign states accountable for tortious actions that occur in the United States, regardless of the medium or method used to commit the tortious action.

Moreover, the proposed location test does not exceed the current statutory language; rather, it falls squarely within the plain text of the rule because it focuses on at least a portion of where the tortious action occurs and the entirety of where is felt. The incorporation of due process principles into the FSIA also finds support in the Act's legislative history. The legislative history shows Congress clearly intended for due process protections to apply to some agencies and instrumentalities of foreign states.[179] Although the expressed intent of Congress in favor of some due process protections does not mean that each FSIA exception must be extended as far as due process allows, it does suggest that a

178. *See supra* notes 156–165 and accompanying text (discussing *Walden v. Fiore*).

179. *See* H.R. REP. NO. 94-1487, at 29–30 (1976) ("If U.S. law did not respect the separate juridical identities of different agencies or instrumentalities, it might encourage foreign jurisdictions to disregard the juridical divisions between different U.S. corporations . . . ."); *see also Bancec*, 462 U.S. 611, 626–27 (1983) ("[G]overnment instrumentalities established as juridical entities distinct and independent from their sovereign should normally be treated as such. We find support for this conclusion in the legislative history of the Foreign Sovereign Immunities Act.").

jurisdictional doctrine that fits within due process principles is consistent with Congress's intent. Additionally, courts have applied or referred to due process principles to determine whether the statutory nexus requirements of other FSIA exceptions have been met.[180]

Determining the situs of cyber torts in the way proposed by this Note is a straightforward test, the elements of which will be familiar to courts, who already apply the *Calder*-*Walden* framework. Given that courts are already familiar with the basic elements of the proposed location test, it will be easier for courts to adopt this approach than to interpret a new and unfamiliar statute. Finally, the proposed test ensures that foreign states are held accountable for their tortious behavior that is directed at the United States and simultaneously continues to adhere to the U.S. approach to foreign sovereign immunity.

CONCLUSION

The rapid evolution of technology has brought with it unprecedented advancements in fields such as medicine, renewable energy, and artificial intelligence, along with the ability for businesses to operate across the world instantaneously. Unfortunately, the rapidly changing world of technology has also introduced new ways to violate legally recognized rights—chief among them the cyber tort. Cyber torts raise a host of novel legal concerns, which are further complicated when such tortious activity is committed by a foreign state. Given the increased prevalence of such torts, including several believed to be attributable to foreign states,[181] it is imperative that U.S. courts articulate how such actions will be treated.

The noncommercial tort exception to the FSIA provides an answer to this conundrum. Through its proposed location test, this Note argues for an interpretation of this exception that allows victims of cyber torts to file suit against responsible foreign sovereigns in U.S. courts. Rather than foreclose the possibility of redress to cyber tort victims, as the D.C. Circuit effectively did in *Doe*,[182] courts should instead interpret the "occurring in the United States" requirement to

180. *See, e.g.*, Triple A Int'l, Inc. v. Democratic Republic of the Congo, 721 F.3d 415, 418 (6th Cir. 2013) (Merritt, J., concurring) (relying on the FSIA's legislative history to conclude that the defendant did not have sufficient minimum contacts with the United States to confer jurisdiction); Terenkian v. Republic of Iraq, 694 F.3d 1122, 1137 (9th Cir. 2012) (viewing the minimum contacts analysis as analogous to determining the applicability of the FSIA's commercial activity exception); BP Chems. Ltd. v. Jiangsu Sopo Corp., 420 F.3d 810, 818 (8th Cir. 2005) (holding that satisfaction of the commercial activity exception disposes of the issue whether the defendant had sufficient minimum contacts with the forum).

181. *See supra* notes 15–19 and accompanying text.

182. *See supra* Section II.D (discussing *Doe v. Federal Democratic Republic of Ethiopia*).

be satisfied when (1) the foreign state intentionally committed the act, (2) the act was expressly aimed at the United States, and (3) the foreign state knew or should have known that the injury would be felt in the United States. If this suggested interpretation is adopted, victims of cyber torts will have an avenue through which to pursue civil redress against foreign states who perpetrate them. This result furthers Congress's purpose in drafting exceptions to the FSIA yet is narrow enough to protect the United States from significant reciprocity concerns.

*Samantha N. Sergent**

* J.D. Candidate, 2019, Vanderbilt University Law School; B.A., 2013, Boston University. First, thank you to Professor Ingrid Wuerth; without her encouragement and guidance, this Note would not have been possible. Thank you to the editors and staff of the *Vanderbilt Law Review* for their hard work and dedication. Finally, thank you to my friends and family—especially my parents, Dave and Cyndi, and my sisters, Kate and Tori—without whose unwavering support I would not be where I am today.