FOREIGN RELATIONS LAW — SOVEREIGN IMMUNITY — D.C. CIRCUIT FINDS ETHIOPIA IMMUNE IN HACKING SUIT. — *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017), *reh'g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

Nation-state hacking is fashionable: everyone is doing it,[1] and everyone wants a say in its regulation.[2] Recently, in *Doe v. Federal Democratic Republic of Ethiopia*,[3] the D.C. Circuit turned back an effort to hold an intelligence service accountable in tort for one of its intrusions. Confronted with a claim that Ethiopia had deployed malware to monitor a Maryland resident's home computer, the court found the suit barred by the Foreign Sovereign Immunities Act of 1976[4] (FSIA), which provides "the sole basis for obtaining jurisdiction over a foreign state" in American courts.[5] The court squarely rejected the plaintiff's effort to invoke in a novel context one of the Act's few limits on immunity, the noncommercial tort exception.[6] That caveat governs all cases of "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 [a] foreign state,"[7] though it was drafted with diplomats' traffic accidents foremost in mind.[8] To an extent, then, the instinct to deny recovery makes good sense; tort is not a counterintelligence regime, and suits like *Doe* are awkward vehicles for espionage anxieties. But the panel's framework — a cramped understanding of whether the tort occurred in the United States — is an awkward fit in its own right. *Doe*'s spatial analysis is tangled, squares poorly with the text and purpose of the FSIA, and marks a significant twist on precedent. When facing new spying suits, other circuits looking to dismiss should look for other tools.

Kidane (a pseudonym, used here and throughout the suit[9]) was born in Ethiopia but found asylum in the United States in the 1990s.[10] From

---

1 *See, e.g.*, Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017, 6:00 AM), https://www.wired.com/story/russian-hackers-attack-ukraine/ [https://perma.cc/74XM-VL9B]; Mike Ives & Paul Mozur, *Small Countries' New Weapon Against Goliaths: Hacking*, N.Y. TIMES (May 14, 2017), https://nyti.ms/2qgY8aX [https://perma.cc/FT5M-DNRP].

2 *See, e.g.*, Andrew Crocker, *What to Do About Lawless Government Hacking and the Weakening of Digital Security*, ELECTRONIC FRONTIER FOUND. (Aug. 1, 2016), https://www.eff.org/deeplinks/2016/08/what-do-about-lawless-government-hacking-and-weakening-digital-security [https://perma.cc/9KTH-739Y]; Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT: ON ISSUES (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ [https://perma.cc/5L6V-BNK9].

3 851 F.3d 7 (D.C. Cir. 2017), *reh'g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

4 Pub. L. No. 94-583, 90 Stat. 2891 (codified as amended in scattered sections of 28 U.S.C.).

5 Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 434 (1989).

6 *Doe*, 851 F.3d at 9–11.

7 28 U.S.C. § 1605(a)(5) (2012).

8 *Amerada Hess*, 488 U.S. at 439–40.

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

10 Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp. 3d 6, 9 (D.D.C. 2016).

his Maryland home, he apparently drew the attention of Ethiopian intelligence by dint of his support for human rights activists in the diaspora.[11] Among the human rights abuses of which Ethiopia is commonly accused: extralegal surveillance.[12] From late 2012 through spring 2013, Ethiopia allegedly monitored Kidane via a commercial spyware application — FinSpy — that had infected his home computer.[13] The program had been delivered in an email forwarded to Kidane, though the message's exact point of origin was a question that remained unclear throughout the litigation.[14] A 2013 investigation by the University of Toronto's Citizen Lab revealed, however, that the instance of FinSpy on Kidane's device was communicating with a server in Ethiopia.[15]

Discovering as much, Kidane sued in the U.S. District Court for the District of Columbia, alleging intentional intrusion upon his seclusion — a Maryland tort — and a violation of the Wiretap Act.[16] Ethiopia raised as its chief shield the FSIA,[17] arguing that Kidane's claims couldn't fit through the noncommercial tort exception. The district court agreed and dismissed.[18] As Judge Moss explained, the circuit applies the exception only if the "entire tort," including "not only the injury but also the act precipitating that injury," took place in the United States.[19] Here,

---

[11] Opening Brief for Appellant John Doe at 3–4, *Doe*, 851 F.3d 7 (No. 16-7081), https://www.eff.org/files/2016/10/24/opening_brief_of_appellant_kidane_v._ethiopia.pdf [https://perma.cc/8JTA-TBUL].

[12] *See generally* HUMAN RIGHTS WATCH, "THEY KNOW EVERYTHING WE DO": TELECOM AND INTERNET SURVEILLANCE IN ETHIOPIA (2014), https://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf [https://perma.cc/FL8Q-5RXR].

[13] Opening Brief for Appellant John Doe, *supra* note 11, at 5.

[14] *See Doe*, 189 F. Supp. 3d at 21.

[15] Opening Brief for Appellant John Doe, *supra* note 11, at 5–6; *see* Morgan Marquis-Boire et al., *You Only Click Twice: FinFisher's Global Proliferation*, CITIZEN LAB (Mar. 13, 2013), https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ [https://perma.cc/U9N2-XJTW].

[16] *Doe*, 189 F. Supp. 3d at 10–11; *see* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 211 (codified as amended at 18 U.S.C. §§ 2510–2520 (2012)).

[17] *Doe*, 189 F. Supp. 3d at 11. Ethiopia also argued that the Wiretap Act "does not provide a cause of action against a foreign state." *Id.* While the district court agreed, *id.* at 15, the D.C. Circuit disclaimed any need to reach the question, *Doe*, 851 F.3d at 9. Nor did the panel revisit defenses rejected below: that Kidane failed to allege a plausible injury, that he alleged a tort covered by a caveat for "misrepresentation" or "deceit," and that he alleged conduct immunized by the discretionary function exception. *Doe*, 189 F. Supp. 3d at 17; *see Doe*, 851 F.3d at 9 n.3.

[18] *Doe*, 189 F. Supp. 3d at 9.

[19] *Id.* at 19 (quoting Jerez v. Republic of Cuba, 775 F.3d 419, 424 (D.C. Cir. 2014)). While on its face the FSIA requires only that the plaintiff's injury occur in the United States, *see* Persinger v. Islamic Republic of Iran, 729 F.2d 835, 844 (D.C. Cir. 1984) (Edwards, J., dissenting in part and concurring in part), every circuit to address the question has required a domestic act, *see* O'Bryan v. Holy See, 556 F.3d 361, 382 (6th Cir. 2009); Cabiri v. Government of the Republic of Ghana, 165 F.3d 193, 200 n.3 (2d Cir. 1999); Jones v. Petty-Ray Geophysical, Geosource, Inc., 954 F.2d 1061, 1065 (5th Cir. 1992); Frolova v. USSR, 761 F.2d 370, 379 (7th Cir. 1985) (per curiam); Olsen *ex rel.* Sheldon v. Government of Mexico, 729 F.2d 641, 645 (9th Cir. 1984). This interpretation turns on expressions of such a requirement in legislative history. *See, e.g.*, *Persinger*, 729 F.2d at 843 (quoting

Judge Moss reasoned, at least some and possibly all relevant acts took place abroad.[20] That decision was backed by a reluctance to disrupt the balance the FSIA strikes between citizens' redress and international comity,[21] to risk discord or even "foreign government retaliation."[22]

The D.C. Circuit affirmed,[23] though with substantially less focus on questions of novelty or comity. Writing for the panel, Judge Henderson[24] held that both of Kidane's claims flunked the entire-tort test.[25] Though the court did not offer a generally applicable account of what constitutes a "tort" for entire-tort purposes, it identified two "integral aspects of the final tort" that fell abroad in Kidane's case.[26] First, the court insisted that "the tortious intent aimed at Kidane,"[27] whose exact location it didn't pin down,[28] "plainly lay abroad."[29] Second, the court said, "FinSpy's initial deployment" occurred abroad.[30] The panel didn't purport to locate this event with precision either, but Kidane had never

---

H.R. REP. NO. 94-1487, at 21 (1976), *as reprinted in* 1976 U.S.C.C.A.N. 6604, 6619). But the Supreme Court has never squarely addressed the question. While it suggested in *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428 (1989), that the exception requires a domestic tort, *id.* at 441, the Court is keen on plain meaning these days, *see, e.g.*, Brett M. Kavanaugh, *Fixing Statutory Interpretation*, 129 HARV. L. REV. 2118, 2118 (2016) (book review) ("As Justice Kagan recently stated, 'we're all textualists now.'").

20 *Doe*, 189 F. Supp. 3d at 21.

21 *See id.* at 23–24.

22 *Id.* at 23 (quoting *Persinger*, 729 F.2d at 841).

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

24 Judge Henderson was joined by Senior Judge Sentelle and Judge Wilkins.

25 *Doe*, 851 F.3d at 11. The court also squarely rejected Kidane's effort to invoke a hypothetical broached in one of its recent precedents, *Jerez v. Republic of Cuba*, 775 F.3d 419 (D.C. Cir. 2014). There, a plaintiff whom Cuban torturers had allegedly infected with hepatitis C attempted to argue that "a separate tort occurred each time the virus replicated in his body" and thus that the defendants committed torts entirely within the United States after he relocated there. *Doe*, 851 F.3d at 10. He "analogiz[ed] the defendants' actions to a foreign agent's delivery into the United States of an anthrax package or a bomb," to which the court, disagreeing, replied that in fact "the defendants' infliction of injury . . . occurred entirely in Cuba, whereas the infliction of injury by the hypothetical anthrax package or bomb would occur entirely in the United States." *Id.* (alteration in original) (quoting *Jerez*, 775 F.3d at 424). This remark seemed to speak directly to Kidane's allegation; the court, however, disclaimed it as dicta before proceeding to the analysis that follows. *Id.*

26 *Doe*, 851 F.3d at 11. The court did, however, refuse to frame the question in terms of the "gravamen" of the tort, *id.* at 12 (quoting OBB Personenverkehr AG v. Sachs, 136 S. Ct. 390, 396 (2015)), or the "'point of contact' between the tort and its victim," *id.* at 11 (quoting *Sachs*, 136 S. Ct. at 397). Kidane drew this language from interpretations of the FSIA's exception for commercial torts — to which the court replied 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." *Id.* at 12 (first quoting *Sachs*, 136 S. Ct. at 396; then quoting Asociacion de Reclamantes v. United Mexican States, 735 F.2d 1517, 1525 (D.C. Cir. 1984) (Scalia, J.) (emphasis added)).

27 *Id.* at 10.

28 *Id.* (noting the same result would obtain whether the intent lay "in London [where the individual who sent the infected email to Kidane may have been], Ethiopia or elsewhere").

29 *Id.*

30 *Id.* at 11.

alleged that the email infected with FinSpy originated in the United States.[31]

In explaining what made these two points "integral," the court seemed to suggest a causal inquiry, noting that "[w]ithout the software's initial dispatch or an intent to spy . . . Ethiopia could not have intruded upon Kidane's seclusion" or violated the Wiretap Act.[32] For the panel, this observation defeated Kidane's effort to analogize his case to two suits that involved assassins directed from abroad: *Liu v. Republic of China*[33] and *Letelier v. Republic of Chile*.[34] Those cases stood, Kidane had argued, for the proposition that the entire-tort inquiry does not ask where an alleged wrong "was planned, commanded, or directed."[35] But while those suits may have featured some foreign facts, the court stressed, they also "involved actions 'occurring in the United States' that were — *without reference to any action undertaken abroad* — tortious."[36] In other words, the *Letelier* and *Liu* complaints would still recount complete wrongs — murders — if every reference to conduct abroad were excised. The allegations in *Doe*, by comparison, would have narrative holes where wrongful intent and the story of the spyware's origins should be. Kidane would be left to complain of the bare fact of FinSpy sitting on his computer, siphoning his emails and calls.[37]

The court was not much taken with Kidane's argument that this outcome clashed with the FSIA's legislative history. He had pointed out that Congress considered — but did not for one reason or another adopt — the European Convention on State Immunity's requirement that "the author of the injury or damage [be] present in that territory at the time" of the tort if immunity is to be abrogated.[38] Without per se embracing that requirement itself, the panel disputed whether dismissal

---

[31] Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp. 3d 6, 21 (D.D.C. 2016).

[32] *Doe*, 851 F.3d at 11. The court also suggested intent is "integral" because it forms an element of both torts, though the court did not conduct an element-by-element analysis. *See id.* at 10–11.

[33] 892 F.2d 1419 (9th Cir. 1989).

[34] 488 F. Supp. 665 (D.D.C. 1980).

[35] Final Reply Brief of Appellant at 5, *Doe*, 851 F.3d 7 (No. 16-7081), https://www.eff.org/files/2017/01/03/12.27.16_final_reply_brief_of_appellant_john_doe.pdf [https://perma.cc/PK5S-6EJN]; *see also* Opening Brief for Appellant John Doe, *supra* note 11, at 25–27.

[36] *Doe*, 851 F.3d at 11 (emphasis added).

[37] The court did not explicitly engage with Kidane's argument that such a complaint should suffice — that having alleged intentional interception, he made out a claim without reference to where the spyware originated. *See* Final Reply Brief of Appellant, *supra* note 35, at 11–13 ("[T]he tort alleged here is not the sending of the email, but rather the activation and maintenance of the spyware." *Id.* at 13.). The panel's opinion is probably best understood as embracing Ethiopia's argument that "[d]evices do not act; persons do." Final Brief for Appellee at 16, *Doe*, 851 F.3d 7 (No. 16-7081), https://www.eff.org/files/2017/01/03/12.28.16_final_brief_for_appellee_ethiopia.pdf [https://perma.cc/25HF-DV7B]. In that light, the court *had* to look for conduct abroad in defining the tort. There were, excluding FinSpy from the stage, no acts in the United States to point to.

[38] *Doe*, 851 F.3d at 11 (quoting European Convention on State Immunity art. 11, May 16, 1972, 1495 U.N.T.S. 181, 185).

was really so dissonant with the intent of the drafters, observing that the "primary purpose" of the exception "was to eliminate a foreign state's immunity for traffic accidents."[39] The court also noted in a footnote that "when the State Department Legal Adviser was asked whether there was any inconsistency between the European Convention and the FSIA, he responded that . . . there generally was not";[40] *Doe* leaves a shade unclear whether the court would adopt that suggestion wholesale. Ultimately, where the district court had seen a "close"[41] and original[42] question, the D.C. Circuit thought its own concise findings "unsurprising."[43]

Even if sound intuition called for dismissal, though, the court's nonchalance is too pat. *Doe*'s reasoning has significant internal tensions and, more to the point, creates tension with the text and aims of the FSIA. The intent requirement is a departure from precedent, one the court fails to justify; the panel's analysis of the scope of the entire tort lacks a clear limiting principle; and its innovations on both points implicate questions of foreign relations better addressed by the political branches.

Consider first the court's analysis of intent. Though Ethiopia had certainly argued that its alleged tortious intent was formulated abroad,[44] the parties might justifiably have been surprised to see the court rest its holding on that point. The alleged situs of intent figured in none of the circuit's entire-tort precedents, nor does the situs of intent appear in the tort exception precedents of other circuits.[45] And for good reason. The statutory language doesn't ask about the tortfeasor's intent; it requires only an "injury . . . occurring in the United States and caused by the tortious act or omission of [a] foreign state."[46] The idea that intent has a situs at all is somewhat strange on its face.[47] If intent is located where intentional acts are located, the requirement is duplicative; if intent is located where intentional tortfeasors are located, *Doe*'s analysis establishes an actual presence requirement, a significant development that

---

[39] *Id.* (quoting Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 439 (1989)).

[40] *Id.* at 11 n.6.

[41] Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp. 3d 6, 21 (D.D.C. 2016).

[42] *Id.* at 19 n.5 ("Neither party cites any decisions applying the FSIA's non-commercial tort exception to torts facilitated by the Internet and directed from abroad.").

[43] *Doe*, 851 F.3d at 11.

[44] Final Brief for Appellee, *supra* note 37, at 5.

[45] *See* cases cited *supra* note 19; *cf.* Stephen J. Schultze, Note, *Hacking Immunity: Computer Attacks on United States Territory by Foreign Sovereigns*, 53 AM. CRIM. L. REV. 861, 877–79, 889 (2016) (arguing that a test asking where the tortfeasor's injurious intent is *directed* "is easily reconciled with existing case law," *id.* at 877, and would resolve *Doe* in Kidane's favor).

[46] 28 U.S.C. § 1605(a)(5) (2012).

[47] *Cf.* Felix S. Cohen, *Transcendental Nonsense and the Functional Approach*, 35 COLUM. L. REV. 809, 824–29 (1935) (criticizing reliance on spatial fictions in answering substantive policy questions). One argument against the entire-tort rule might proceed from the point that "omissions" are similarly hard to locate. *See* Doe v. Holy See, 434 F. Supp. 2d 925, 953 (D. Or. 2006).

would deserve a clear statement.[48] *Doe* could be read to stand for either of these propositions, in part because neither is convincingly justified.

At minimum, imposing an actual presence requirement requires a more careful study of statutory purpose than *Doe* undertook. As Judge Moss acknowledged, "Ethiopia's alleged surveillance would fall squarely within the 'entire tort' rule had it sent a 'flesh-and-blood agent into [Kidane's] house to install a recording device.' Technology has simply rendered the human agent obsolete."[49] Given that the rationale for imposing the entire-tort rule turns on congressional intent — the text does not require it[50] — it seems appropriate to ask whether Congress meant to attach significance to that distinction. The answer is at least ambiguous. The strongest case in favor would be the one that Ethiopia mounted: international law favors the actual presence requirement,[51] and the FSIA was broadly intended to codify international law.[52] Of course, this fails to explain the absence of the requirement from the plain text. It bears mentioning, too, that Congress recently chose to challenge the international law of immunity on just this point. Passed over fierce objections from scholars[53] and the executive branch,[54] the Justice Against Sponsors of Terrorism Act[55] (JASTA) rejects any requirement that suits within its reach allege even *one* domestic tortious act.[56] Whether that rule is wise or not, such immunity questions — especially one as ambiguous as the actual presence requirement — "inherently involve[] a political judgment"[57] better left to a representative branch.

The court's analysis of the acts that make up the tort has similar problems. As with intent, the panel's decision to focus on the spyware's dispatch was made in a precedential vacuum.[58] Courts haven't faced

---

48 Indeed, Ethiopia went so far as to argue that this was the *point* of the entire-tort rule. Final Brief for Appellee, *supra* note 37, at 24. No court has signaled as much. *See* cases cited *supra* note 19.

49 Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp. 3d 6, 20 (D.D.C. 2016) (alteration in original) (citation omitted).

50 *See supra* note 19.

51 *See* European Convention on State Immunity art. 11, May 16, 1972, 1495 U.N.T.S. 181, 185.

52 *See generally* H.R. REP. NO. 94-1487 (1976), *as reprinted in* 1976 U.S.C.C.A.N. 6604.

53 *See, e.g.*, Curtis Bradley & Jack Goldsmith, Opinion, *Don't Let Americans Sue Saudi Arabia*, N.Y. TIMES (Apr. 22, 2016), https://nyti.ms/2k7Mmgu [https://perma.cc/WG7R-APBM].

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

55 Pub. L. No. 114-222, 130 Stat. 852 (2016) (to be codified at scattered sections of 18 and 28 U.S.C.).

56 *Id.* sec. 3, § 1605B(b)(2), 130 Stat. at 853.

57 Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp. 3d 6, 24 (D.D.C. 2016).

58 Certainly there was no consensus in academic commentary. *See* Schultze, *supra* note 45, at 885–86 (suggesting the district court in *Doe* might find the entire-tort rule satisfied *vel non*, or find it wholly inapplicable); *see also* Paige C. Anderson, Note, *Cyber Attack Exception to the Foreign Sovereign Immunities Act*, 102 CORNELL L. REV. 1087, 1096 (2017). Scott Gilmore, who represented Kidane, argues that "courts generally apply the tort exception whenever a substantial part of the acts or omissions occurs in the United States." Scott A. Gilmore, *Suing the Surveillance*

pressure to define an act's nature or a tort's scope with specificity: most entire-tort precedents deal with courses of conduct that took place *entirely* outside the United States.[59] But the question has stakes. As the Ninth Circuit recognized in *Olsen ex rel. Sheldon v. Government of Mexico*,[60] defining the scope of an "entire tort" too broadly incentivizes states to dodge suit by pleading collateral acts abroad.[61] Such a regime would threaten statutory purpose. It is "hardly likely" that Congress intended the FSIA to immunize, say, letter-bomb campaigns so long as "a country plotting a political murder in the United States were to take steps to ensure that some small part of the wrongful act . . . took place abroad."[62] But *Doe* suggests such a result obtains in hacking cases, and its framework is vague enough that it may undermine the inquiry elsewhere.

After all, the D.C. Circuit's designated "precipitating act" is fairly remote from the alleged injury. The court's emphasis on the spyware's transmission would do more to limit the scope of the analysis if the infected email had been sent directly to Kidane; instead, it was delivered via a third party whose role none involved seemed to fully understand.[63] Similarly, it might have been easy enough to identify a unique precipitating act if a keystroke in Ethiopia were required to intercept Kidane's communications after infection. Here, though, FinSpy operated automatically after taking root,[64] and the court seems to have been reluctant to characterize FinSpy's operations as "acts" attributable to Ethiopia.[65] Future courts are left to guess what standard *Doe* applied in choosing to incorporate transmission into the "entire tort." Was it the proximate cause?[66] A but-for cause? The last significant act?[67] Kidane, for his

---

States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act, 46 COLUM. HUM. RTS. L. REV. 227, 254 (2015). This is a bold reading of the case law. *See supra* note 19.

[59] *See* Schultze, *supra* note 45, at 873.

[60] 729 F.2d 641 (9th Cir. 1984).

[61] *Id.* at 646.

[62] Joseph W. Dellapenna, *Refining the Foreign Sovereign Immunities Act*, 9 WILLAMETTE J. INT'L L. & DISP. RESOL. 57, 137 (2001) (describing concerns of the ABA's Working Group on the FSIA). JASTA's legislative history suggests lawmakers would share this anxiety, if not this understanding. *See* Press Release, House Comm. on the Judiciary, S.2040, the *Justice Against Sponsors of Terrorism Act* (JASTA) (Sept. 2016), https://lamborn.house.gov/uploadedfiles/jasta_veto_override_-_one_pager-v1.pdf [https://perma.cc/F5JM-DRRQ] (taking the entire-tort rule to mean that, "[u]nder the FSIA, as currently written, a country that sponsors a terrorist attack against the United States could escape liability if *all* of the support it provided occurred overseas" (emphasis added)).

[63] *See Doe*, 851 F.3d at 8.

[64] Opening Brief for Appellant John Doe, *supra* note 11, at 15.

[65] *See supra* note 37.

[66] Interpreting the FSIA's "terrorism exception," the D.C. Circuit has held that the words "caused by" require plaintiff to show proximate causation as part of the jurisdictional burden. Kilburn v. Socialist People's Libyan Arab Jamahiriya, 376 F.3d 1123, 1128 (D.C. Cir. 2004).

[67] *Cf.* Sosa v. Alvarez-Machain, 542 U.S. 692, 759–60 (2004) (Ginsburg, J., concurring in part and concurring in the judgment) (proposing that, for purposes of the Federal Tort Claims Act, courts should resolve whether a tort "aris[es] in a foreign country," 28 U.S.C. § 2680(k) (2012), by asking where the "last significant act" occurred).

part, argued in his petition for rehearing en banc that *Doe* had expanded the entire-tort inquiry to embrace "merely preparatory acts."[68] In that light, the entire-tort rule, as elaborated in *Doe*, threatens to become overstrong medicine in the effort to foreclose antihacking suits.

None of this is to say foreclosing recovery would be unwise. Abrogating immunity may well pose diplomatic risks and would certainly constrain the United States in any effort to set international norms on hacking. After all, the FSIA is meant to play a harmonizing function, "to subject foreign states that commit torts in the United States to the same rules of immunity applied against the United States abroad."[69] And as one of Kidane's attorneys acknowledged, "[e]ven if such claims do not directly implicate the legality of U.S. surveillance, they may risk exposing the United States to reciprocal treatment in the courts of foreign countries."[70] The United States would hardly favor a global rule of no-immunity for an activity in which it engages with at least as much enthusiasm — and often more — than any other state.[71] Nor is hacking for intelligence or law enforcement ends so obviously wrongful that the United States should lend its courts' weight to stigmatizing the habit.[72]

Contra suggestions that Congress should smooth the way for spying suits,[73] then, lawmakers might want to block such claims more clearly than the entire-tort rule does. But certainly other circuits, in light of the strain *Doe* places on the noncommercial tort exception, should be wary of embracing its approach to the inquiry. There may well be better tools if courts hope to exclude these suits; Kidane for one seemed concerned that the political question and act of state doctrines had underpinned the district court's reasoning.[74] Ultimately, though, whether or not these approaches would shut the door to hacking suits, and whether or not abrogating immunity here might have consequences not anticipated by the lawmakers who drafted the FSIA, Congress "did not confer common law authority on the courts to *adjust* the rules of foreign sovereign immunity to new and unanticipated events that might arise."[75] In stretching the (already judge-made) entire-tort rule to new lengths, *Doe* highlights the thickets into which those adjustments can plunge the courts.

---

[68] Appellant John Doe's Petition for Rehearing *En Banc* at 2, *Doe*, 851 F.3d 7 (No. 16-7081), https://www.eff.org/files/2017/04/13/2017-04-13_petition_dckt_.pdf [https://perma.cc/J2ZH-BD8Z].

[69] Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp. 3d 6, 24 (D.D.C. 2016).

[70] Gilmore, *supra* note 58, at 276.

[71] *See, e.g.*, Dan Goodin, *How "Omnipotent" Hackers Tied to NSA Hid for 14 Years — and Were Found at Last*, ARS TECHNICA (Feb. 15, 2015, 2:00 PM), https://arstechnica.com/?post_type=post&p=613403 [https://perma.cc/7DAZ-8PF3].

[72] *See generally* Orin S. Kerr & Sean D. Murphy, Essay, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58 (2017); Beatrice A. Walton, Note, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law*, 126 YALE L.J. 1460, 1474 (2017).

[73] *See generally* Anderson, *supra* note 58.

[74] Opening Brief for Appellant John Doe, *supra* note 11, at 30–33.

[75] Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp. 3d 6, 24 (D.D.C. 2016).