ORAL ARGUMENT HELD FEBRUARY 2, 2017

No. 16-7081

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

JOHN DOE, A.K.A. "KIDANE",

Plaintiff-Appellant,

v.

FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA,

Defendant-Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPELLANT JOHN DOE'S PETITION FOR REHEARING *EN BANC*

Nathan Cardozo Cindy Cohn ELECTRONIC FRONTIER FOUNDATION 815 Eddy Street San Francisco, CA 94109 (415) 436-9333	Richard M. Martinez JONES DAY 90 South Seventh Street, Suite 4950 Minneapolis, MN 55402 (612) 217-8800
Samuel L. Walling ROBINS KAPLAN LLP 800 LaSalle Avenue, Suite 2800 Minneapolis, MN 55402 (612) 349-8500	Scott A. Gilmore CENTER FOR JUSTICE & ACCOUNTABILITY One Hallidie Plaza, Suite 406 San Francisco, CA 94102 (415) 544-0444

Counsel for Appellant John Doe

STATEMENT PURSUANT TO FED. R. APP. P. 35(b)

A panel of this Court has rendered an alarming ruling that tears a gaping hole in the Foreign Sovereign Immunities Act ("FSIA"), leaving American citizens and businesses exposed to foreign states that use modern technology to remotely execute serious torts within the United States. It thus raises the critically important question of whether, in this time of increasing cyber threats from abroad, foreign states may enjoy immunity from suit simply by leveraging fundamental technologies like the internet, and quickly-evolving technologies like drones, to engage in certain activities on our territory albeit without their human agents being physically present on our territory.

This case arises from Ethiopia using computer malware to infect Appellant Kidane's home computer in Maryland, and to wiretap and monitor both him and his family. The panel held that Ethiopia is immune from suit because its "digital espionage" did not fall within the noncommercial tort exception to the FSIA. Panel Opinion (Op.) at 7. Focusing on the fact that Ethiopia formed the *intent* to wiretap Kidane's home computer and to intrude upon his seclusion, abroad, the panel held that Kidane had alleged a "transnational tort" that did not occur entirely within the United States. *Id.* at 2.

The panel's decision conflicts with this Court's ruling in *Jerez v. Republic of Cuba*, 775 F.3d 419 (D.C. Cir. 2014), which held that the noncommercial tort

exception applies when (1) the injury, and (2) the act precipitating the injury occur in the United States. The undisputed facts establish that Ethiopia's digital agent, the FinSpy malware program installed on Kidane's computer, intercepted Kidane's communications and intruded upon his seclusion in Maryland. In looking past these acts to other, merely preparatory acts that occurred abroad, the panel not only misapplied *Jerez*, but also reached a decision that conflicts the Supreme Court's holding in *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 439 (1989), which did not set forth an element-by-element analysis or create an all-elements rule.

The panel's decision also conflicts with this Court's ruling in *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013), which held that a violation of the Wiretap Act occurs at the site of interception. The panel held that "at least a portion" of the torts Kidane alleged occurred abroad. Op. at 6. This result disregards the undisputed fact that the entirety of the alleged interception occurred in Maryland, meaning that the violation of the Wiretap Act occurred in Maryland.

In addition, the panel's decision raises a question of exceptional importance because it greivously injures the purpose of the FSIA, which is to "serve the interests of justice and . . . protect the rights of both foreign states and litigants in United States courts." 28 U.S.C. § 1602. Left unaltered, the panel's decision establishes that foreign states are immune from suit for torts executed within the

United States, so long as no human agent is physically present in the United States. Thus, foreign states would be free to unleash cyberattacks that steal personal data, damage property or injure people, and even seize control of cars that belong to political opponents who live in this country or have sought refuge here. That technology such as the internet allows foreign states to accomplish these—and numerous other—serious torts intentionally from abroad should be of little import if the FSIA is to continue to protect the rights of Americans to seek relief from United States courts in the Digital Age.

STATEMENT OF THE CASE

This case began when Kidane filed suit in the United States District Court for the District of Columbia, alleging that Ethiopia had used a commercially-available sophsiticated software program called FinSpy to intercept his Skype telephone calls and to monitor his online activities. JA 430. A report from the University of Toronto's Munk Shool of Global Affairs, relvealed that Ethiopia used FinSpy to surveil Ethiopian political oppoenents living abroad. JA 436-443. A forensic analysis demonstrated that Kidane's computer had been infected with FinSpy, and that the program had secretly recorded his calls and computer usage, and had coding instructions for sending activity logs to the same Ethiopian-based FinSpy server identified in the University of Toronto's report. JA 443-448.

The district court dismissed Kidane's suit, holding *inter alia* that Ehiopia was immune because the FSIA's noncommercial tort exception did not apply. JA 666. Kidane sought review and a panel of this Court affirmed. JA 702; Addendum. The panel held that the noncommercial tort exception did not apply because Kidane had failed to allege facts showing that the "entire tort" occurred in the United States. Op. at 7-8. The panel paid little attention to the fact that the alleged infection and interception occurred in the United States. Instead, the panel noted that the "intent aimed at Kidane" and "the tortious acts of computer programming" lay abroad. *Id*. at 6-7. The panel further noted that the "initial deployment" of the FinSpy software (sending an e-mail) occurred abroad. *Id.* at 7. Thus, the panel concluded that the torts alleged "did not occur 'entire[ly]' in the United States." *Id.*

ARGUMENT

I. THE PANEL'S DECISION CONFLICTS WITH THIS COURT'S *JEREZ* TEST FOR DETERMINING WHETHER THE FSIA'S NON-COMMERCIAL TORT EXCEPTION APPLIES

In *Jerez v. Republic of Cuba*, this Court clearly enunciated the test for determining whether an "entire tort" occurred in the United States for the purposes of the FSIA's non-commercial tort exception. 775 F.3d at 424, (interpreting *Amerada Hess*, 488 U.S. at 441. The test holds that, in order for the exception to

apply, the two components creating the "entire tort" must occur in the United States. *Id.*; *see also Associacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1525 (D.C. Cir. 1984). These two components are: (1) the injury and (2) the act precipitating that injury. *Id.* at 424.

In *Jerez*, the plaintiff was imprisoned and tortured for many years in Cuba, where he was purposefully injected with the hepatitis C virus. *Id.* at 421. Years later, the plaintiff moved to the United States where he commenced an action against Cuba on the theory that the continuing replication of the virus within his body constituted an ongoing tort. *Id*. This Court held that while the plaintiff indeed suffered *injury* within the United States, the *acts* that precipitated that injury—Cuba's injecting him with a virus in Cuba—did not. Because only his ongoing injury occurred here, his suit was barred by the FSIA. *Id*.

Here, the panel misapplied the precipitating-acts prong of *Jerez's* "entire tort" test. There is no dispute that Kidane's injury occurred entirely within the United States: his privacy was violated in his own living room in Maryland. The sole issue is whether the *tortious act* that precipitated his injury also occurred here. Under the second prong of the *Jerez* test, the acts that precipitate a plaintiff's injury occur in the United States when the "defendants' infliction of injury" on the plaintiff "occur[s] entirely in the United States." *Id.*

The panel disregarded whether Ethiopia's infliction of injury occurred entirely within the United States, and focused instead on whether "at least a portion of Ethiopia's alleged tort occurred abroad." Op. at 6. Finding that the preparatory (but non-tortious[1]) work of creating and sending the FinSpy malware occurred outside the United States, the panel concluded that the noncommercial tort exception did not apply. But preparing an email is not "a portion" of the tort of wiretapping. Nor does it represent the "infliction of injury" with which the *Jerez* test is concerned.

Until now, no court has ever held that a tort did not occur entirely in the United States merely because some non-tortious preparation happened abroad. In fact, the Ninth Circuit cautioned against precisely this type of an approach in *Olsen v. Gov't of Mexico*, 729 F.2d 641, 646 (9th Cir. 1984).[2] Clearly a foreign assassin who books a flight to Washington does not immunize his government against a wrongful death claim by buying the ticket overseas.

[1] As discussed in more detail in Section II below, the only tortious acts at issue here are the interception of Kidane's communications and the intrusion upon his seclusion, both of which occurred in his home in Maryland.

[2] An extreme application of the "entire tort" doctrine that looks to preparatory acts "would encourage foreign states to allege that some tortious conduct occurred outside the United States. The foreign state would thus be able to establish immunity and diminish the rights of injured persons seeking recovery. Such a result contradicts the purpose of the FSIA . . . ." 729 F.2d at 646.

The "entire tort" rule should not be read to such an extreme. It is a judge-made doctrine of the lower courts, never adopted—or even cited—by the Supreme Court in its sole decision on § 1605(a)(5): *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428 (1989). There the Court said that "section 1605(a)(5) covers only torts occurring within the territorial jurisdiction of the United States." *Amerada Hess*, 488 U.S. at 441. But the Court did not say the torts—and all preparatory acts—must occur *entirely* within that territorial jurisdiction.

By examining where the non-tortious preparation occurred, the panel's decision expands the scope of the territorial limitation announced in *Amerada Hess* and the two-part test enunciated in *Jerez*. Instead of inquiring only into where the tortious *act* took place (*see* section II *infra*), the panel looked to the place from which the tortfeasor dispatched commands that preceded the tortious act and the place where the tortfeasor developed its tortious intent. *See* Op. at 7. The panel's failure to apply the *Jerez* test requires that its opinion be vacated.

The panel's failure to apply *Jerez* is evident in the panel's treatment of a hypothetical the *Jerez* court used to illustrate the "entire tort" test. In that hypothetical, foreign agents used the mail to deliver "an anthrax package or bomb" "into the United States." *Jerez*, 775 F. 3d at 424. Unlike the actual facts of *Jerez*, in the hypothetical the *act* that precipitated the injury—the exposure to the virus (also

referred to as the infliction of injury)—and the injury—the anthrax infection—occurred in the United States. *Id.* Thus, the Court noted that the hypothetical would satisfy the entire tort rule while the plaintiff's claim did not. *Id.*

The panel apparently recognized that its opinion was in direct conflict with the *Jerez* court's hypothetical. Op. at 6. But rather than attempt to distinguish the instant facts from that hypothetical, the panel simply noted that the "hypothetical was dictum," and not only disregarded it, but also failed to conduct any inquiry into what the precipitating acts in this case were or where they took place. *Id*.

Because the panel failed to inquire into where the actual tortious acts occurred, and looked instead to where the non-tortious preparation occurred, the panel's conclusion that the "entire tort" did not occur in the United States is in direct conflict with *Jerez* and must be vacated.

II. THE PANEL'S DECISION IGNORES SETTLED LAW FOR DETERMINING THE LOCATION OF THE TORTS ALLEGED

Ethiopia committed tortious acts when its malware, resident and running on the Kidane family computer, intercepted Kidane's communications and recorded Kidane's computer activities (Joint Appendix 430-31). It was these acts in Maryland, and these acts alone, that violated the Wiretap Act and invaded Kidane's privacy.

In finding that the torts to which Kidane was subjected did not occur "entirely" within the United States, the panel made three errors: (1) it ignored

settled Wiretap Act law for determining the location of the violation, (2) it misread Maryland common law regarding intrusion upon seclusion, and (3) it appears to have read additional, nonexistent claims into Kidane's complaint.

First, the panel failed to apply settled law that violations of the Wiretap Act occur at the place where the plaintiff's communications are intercepted. *See, e.g.*, *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013) (holding that a violation of the Wiretap Act lies at the site of interception, *i.e.*, "the property on which the device is . . . installed."); *accord United States v. Ramirez*, 112 F.3d 849, 852 (7th Cir. 1997) ("[A]n interception takes place both where the phone is located . . . and where the scanner used to make the interception is located."). The panel disregarded this law and—without citing any Wiretap Act authority—instead found that "at least a portion" of the torts Kidane alleged occurred abroad. This was error.

Similarly, the panel ignored Maryland common law that locates an intrusion upon seclusion at the place where the intrusion occurred. Under Maryland common law, the focus of this tort is the "intrusion into a private place" and the location of the tort is that private place. *New Summit Assocs. Ltd. P'ship v. Nistle*, 533 A.2d 1350, 1354 (Md. App. 1987). Instead of looking to settled Maryland law, however, the panel focused on the fact that intrusion upon seclusion is an intentional tort, and looked to where Ethiopia developed its intent. Op. at 6. While it is

undoubtedly true that intrusion upon seclusion is an intentional tort, *see e.g.*, *Bailer v. Erie Ins. Exch.*, 687 A.2d 1375, 1380–81 (Md. 1997), the development of that intent was not tortious. Indeed, under Maryland law, the tort began and ended in the "private place" into which Ethiopia intruded: Kidane's home computer in Maryland. The panel cited no Maryland law for the proposition that intrusion upon seclusion occurs (even partially) where the tortfeasor formed its intent; there is no such authority.

Finally, the panel erred by mischaracterizing Kidane's complaint as including a claim for "tortious acts of computer programming," which likely occurred within Ethiopia. Op. at 6-7. Kidane makes no claim for any act of programming, tortious or otherwise. Indeed, Kidane alleges that Ethiopia *purchased* the FinSpy software from a third party, Gamma International Ltd. JA 436-37.

The only torts for which Kidane seeks redress are the *interception* of his communications and the *intrusion* into his private personal computer. Those torts both began and ended in his living room in Silver Spring, Maryland.

By disregarding settled law—and by reading claims into Kidane's complaint that simply aren't there—the panel improperly found that the "entire tort" did not occur in the place where Kidane's communications were intercepted and his seclusion intruded upon.

III. THE PANEL'S DECISION RAISES AN ISSUE OF EXCEPTIONAL IMPORTANCE, IN CREATING A NEW "PHYSICAL PRESENCE" REQUIREMENT FOR FSIA NONCOMMERCIAL TORTS

The panel's decision creates a new requirement for FSIA jurisdiction—a human agent must be physically present within the United States before immunity is waived—thereby limiting the noncommercial tort exception in a way that Congress never intended. *See* Op. at 8. The panel grounded its "physical presence" requirement in neither the text of the FSIA nor any existing authority. Given the ways in which technology allows foreign states to commit torts in the United States *without* the physical presence of a human agent, this Court should not endorse the panel's whole-cloth creation of a new limitation on FSIA jurisdiction.

Congress intended the FSIA to serve, among other goals, a broad remedial purpose: "to ensure 'our citizens . . . access to the courts.'" *Verlinden B.V. v. Cent. Bank of Nigeria*, 461 U.S. 480, 490 (1983) (quoting H.R. Rep. No. 94–1487, at 6). Although the exception was "directed primarily at the problem of traffic accidents" it was "cast in general terms as applying to *all tort actions* for money damages, not otherwise encompassed by section 1605(a)(2), relating to commercial activities." S. Rep. No. 94-1310, 20 (1976) (emphasis added). The reason is straightforward: to ensure that Americans can seek redress at least at the same level as foreigners can seek redress for American torts committed against them.

The FSIA's drafters made it apply generally to all torts not specifically exempted. Consistent with that general scope, they focused on a foreign state's *activities* within the United States—not on their presence in the flesh. In the 1973 FSIA hearings, one of the Act's principal draftsmen, Bruno Ristau testified that the Act aimed to:

> subsume to the jurisdiction of our domestic courts foreign governments and foreign entities who engage in certain activities on our territory to the same extent that the U.S. Government is already at the present time subject to the jurisdiction of foreign courts, when it engages in certain activities on their soil . . . .

Immunities of Foreign States: Hearings on H.R. 3493 Before the Subcomm. on Claims and Governmental Relations of the House Comm. on the Judiciary, 93d Cong., 1st Sess. 29 (1973), 29 (testimony of Bruno Ristau) (hereinafter "1973 Hearings").

In 1976, Congress would have been aware that foreign states can engage in activities on U.S. territory through a variety of instrumentalities—some without the physical presence of a human agent. While the drafters of the FSIA might not have anticipated cyberattacks and malware, they were certainly aware of letter bombs and other remotely detonated devices, which saw a wave of use by state-sponsored terrorist organizations in the 1970s.[3] And remote controlled devices such as

[3] National Consortium for the Study of Terrorism and Responses to Terrorism, *Background Report: Incendiary Devices in Packages at Maryland Government Buildings*, Jan. 7, 2011, at 2, *available at*

unmanned aerial vehicles, *i.e.*, drones, were already in extensive use during the Vietnam War, flying surveillance sorties in foreign sovereign territory.[4] Even traffic accidents—an undisputed concern of the tort exception—are not immune to changing technology. Even in 1971, a truck or other vehicle sent over the border could cause damage. Nothing in the text or history of the FSIA suggests that Congress sought to freeze the FSIA in 1976 and apply it only to the technologies—and torts—of its time. Congress was well aware that new statutory torts would emerge and new technologies could inflict personal injury or property damage deserving of redress.

The panel's rigidly narrow application of the noncommercial tort exception presents an issue of exceptional importance. A foreign state's ability to remotely reach into the United States, and to engage in activites on U.S. territory via different means and instrumentalities has grown dramatically in the last decade. Foreign states are no longer dependent on the physical presence of human agents to conduct (tortious) activities within the United States. Thus, the reach of the panel's holding—and the immunity that it provides—is limited only by what technology enables foreign states to accomplish by remote means, today and in the future.

---

http://www.start.umd.edu/sites/default/files/files/publications/br/Background_Report_2011JanuaryPackageIncendiariesMD.pdf

[4] *See* John F. Keane and Stephen S. Carr, *A Brief History of Early Unmanned Aircraft*, 32 Johns Hopkins Apl Technical Digest No. 3, 568 (2013), *available at* http://www.jhuapl.edu/techdigest/TD/td3203/32_03-Keane.pdf.

Whether it is through malware, unmanned drones, or self-driving cars, foreign states can and do cause injuries to Americans on American soil without a human being present. Foreign states routinely hack into private citizens'—and U.S. companies'—computers and steal personal and business information, or otherwise cause damage. It is already "possible to hack remotely into a car's electronics" and cause a "crash from thousands of miles away." JA687.[5] And in the coming years, foreign states will certainly operate self-driving cars in U.S. territory. The panel's decision provides refuge to these and other acts.

Technology may have rendered the human agent unnecessary, but clearly the foreign state has still engaged in tortious activities in U.S. territory. Thus, the panel's decision raises the crucial question of whether the FSIA's noncommercial tort exception will continue to serve its remedial purpose in a digital age. For that purpose to remain intact, this Court must vacate the panel decision and reject the creation of a new "physical presence" requirement.

CONCLUSION

The panel's opinion has broad and serious implications for the digital—and the physical—security of Americans in their own country and in their own homes. In holding that foreign state's remotely delivered digital agent does not commit an

[5] *See* N.Y. Times, *Security Researchers Find a Way to Hack Cars*, (July 21, 2015), http://bits.blogs.nytimes.com/2015/07/21/security-researchers-find-a-way-to-hack-cars/.

"entire tort" within the United States when it surveils an American *in the United States*, the panel's decision creates a rule granting immunity for governments around the world to wiretap, attack, and even murder Americans on American soil, as long as the instrumentality of those crimes has some foothold in a foreign country. That is not what the FSIA requires. In fact, the law was written with precisely the opposite intent in mind: to ensure that Americans have recourse against foreign governments when they commit serious torts within the United States.

American citizens have a right to privacy and security. Kidane has those rights; indeed by seeking citizenship in the United States he, like so many others, sought to live under a legal system that provides strong protection against harassment and spying, whether based upon his political beliefs or otherwise. In order to preserve these rights, the FSIA must be applied in such a way that foreign states cannot use the internet and other technological advances as a judicially-sanctioned means to surveil Americans in their homes.

For the foregoing reasons, Kidane respectfully requests that the Court vacate the panel's decision and grant rehearing *en banc*.

Dated: April 13, 2017

Respectfully submitted,

/s/ Samuel L. Walling
Samuel L. Walling
ROBINS KAPLAN LLP
800 LaSalle Avenue, Suite
2800 Minneapolis, MN 55402
(612) 349-8500
swalling@robinskaplan.com

Richard M. Martinez
JONES DAY
90 S. Seventh Street, Suite 4950
Minneapolis, MN 55402 (612)
217-8800

Nathan Cardozo
Cindy Cohn
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109 (415)
436-9333

Scott A. Gilmore
CENTER FOR JUSTICE &
ACCOUNTABILITY
One Hallidie Plaza, Suite 406
San Francisco, CA 94102 (415)
544-0444

Counsel for Appellant

ADDENDUM PER CIRCUIT RULE 35(c)

1) Certificate as to Parties, Rulings, and Related Cases

2) Disclosure Statement

3) *John Doe, a/k/a Kidane v. The Federal Democratic Republic of Ethiopia*, No. 16-7081 (D.C. Cir. March 14, 2017) (Opinion and Judgment)

1. CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

A. Parties and Amici

The parties to this appeal are Appellant John Doe, a.k.a. Kidane and Appellee, the Federal Democratic Republic of Ethiopia ("Ethiopia"). David Kaye, United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Maina Kiai, United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, and Michel Forst, United Nations Special Rapporteur on the Situation of Human Rights Defenders participated as amici curiae in support of Kidane.

B. Ruling Under Review

This petition seeks rehearing *en banc* of the March 14, 2017, decision of a panel of this Court (Henderson, J., joined by Wilkins, J., and Sentelle, J.), affirming the dismissal of Kidane's Wiretap Act and Maryland common law claims against Ethiopia, finding that no suit can lie under the Foreign Sovereign Immunities Act, 28 U.S.C. § 1605(a)(5), if any portion of the alleged tort occurred abroad, and that some portion of Ethiopia's eavesdropping on Kidane in his living room in Maryland did occur abroad. *See Doe v. Ethiopia*, No. 16-7081, 2017 WL 971831, slip op. at 6-10. There is no official citation for the decision and order. A copy of the panel's decision is attached as an addendum to this Petition.

C. Related Cases.

There are no related cases on appeal.

2. DISCLOSURE STATEMENT

Appellant is an individual. Amici stated that none have a parent corporation and no publicly held corporation owns 10% or more of the stock of any amicus.

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued February 2, 2017 Decided March 14, 2017

No. 16-7081

JOHN DOE, ALSO KNOWN AS KIDANE,
APPELLANT

v.

THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA,
APPELLEE

Appeal from the United States District Court
for the District of Columbia
(No. 1:14-cv-00372)

Richard M. Martinez argued the cause for the appellant. *Samuel L. Walling*, *Nathan Cardozo*, and *Cindy Cohn* were with him on brief. *Scott A. Gilmore* entered an appearance.

David Kaye was on brief for the *amici curiae* United Nations Human Rights Experts in support of the plaintiff-appellant.

Thomas R. Snider argued the cause for the appellee. *Robert P. Charrow* and *Laura Metcoff Klaus* were with him on brief.

Before: HENDERSON and WILKINS, *Circuit Judges*, and SENTELLE, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* HENDERSON.

KAREN LECRAFT HENDERSON, *Circuit Judge*: Plaintiff John Doe—proceeding pseudonymously as "Kidane"—claims he was tricked into downloading a computer program. The program allegedly enabled the Federal Democratic Republic of Ethiopia (Ethiopia) to spy on him from abroad. He wants to sue the Republic of Ethiopia. But foreign states are immune from suit unless an exception to the Foreign Sovereign Immunities Act (FSIA) applies. Kidane invokes the FSIA's exception for noncommercial torts. We conclude his reliance is misplaced. The noncommercial-tort exception abrogates sovereign immunity for a tort occurring *entirely* in the United States. Kidane, by contrast, alleges a transnational tort. We therefore affirm the district court's dismissal for lack of subject matter jurisdiction.

I. BACKGROUND

Now an American citizen, Kidane was born in Ethiopia.[1] He obtained asylum in the United States in the early 1990s and has at all relevant times lived in Silver Spring, Maryland. There, he has remained active in the Ethiopian community and has maintained contacts who work to increase awareness of corruption and human rights issues in Ethiopia.

As alleged in the complaint, in late 2012 or early 2013, Kidane opened an attachment to an e-mail he received from an acquaintance. The e-mail had been forwarded and was

[1] Because, at this stage, Ethiopia has not disputed the factual basis for our jurisdiction but "challenges only the legal sufficiency of [Kidane's] jurisdictional allegations," we "take [his] factual allegations as true and determine whether they bring the case within" the FSIA's noncommercial-tort exception. *Phoenix Consulting Inc. v. Republic of Angola*, 216 F.3d 36, 40 (D.C. Cir. 2000).

allegedly sent originally by or on behalf of Ethiopia. Kidane's complaint is silent as to whether the individual who sent Kidane the e-mail was located in the United States but the e-mail's text suggests that individual was located in London. *See* Am. Compl. Ex. C ("You took your family to London . . . ."). Once opened, the attachment allegedly infected Kidane's computer with a "clandestine . . . program[] known as FinSpy." Am. Compl. ¶ 4. FinSpy is "a system for monitoring and gathering information from electronic devices, including computers and mobile phones, without the knowledge of the device's user." *Id.* ¶ 6. It is "sold exclusively to government agencies." *Id.* After installation on Kidane's computer, FinSpy "began . . . recording some, if not all, of the activities undertaken by users of the computer," whether Kidane or his family members. *Id.* ¶ 5. It then allegedly communicated with a server in Ethiopia.

Kidane filed suit against Ethiopia, pressing two claims. First, Kidane sought relief under the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, which prohibits "any person [from] intentionally intercept[ing] . . . any wire, oral, or electronic communication[,]" *id.* § 2511(1). Second, Kidane alleged Ethiopia committed the Maryland common law tort of intrusion upon seclusion.

The district court dismissed Kidane's lawsuit in its entirety. *Doe v. Fed. Democratic Republic of Ethiopia*, 189 F. Supp. 3d 6, 28 (D.D.C. 2016). It first concluded that the relevant Wiretap Act provision could not be enforced *via* private lawsuit against a foreign government.[2] *Id.* at 12–15.

[2] The district court reached this issue before addressing subject matter jurisdiction under the FSIA. Although recognizing that ordinarily it must address subject matter jurisdiction first, *Doe*, 189 F. Supp. 3d at 11, it forestalled the jurisdictional inquiry based on *Vermont Agency of Natural Resources v. United States ex rel.*

It next dismissed Kidane's state-law claim for lack of subject matter jurisdiction. *Id.* at 15–28. The district court observed that the FSIA grants all foreign states immunity from suit in American courts, subject to limited enumerated exceptions. *Id.* at 16. Kidane invoked only one—the noncommercial-tort exception. *Id.* The district court found that exception inapplicable because the "entire tort" did not occur in the United States, as required.[3] *Id.* at 18–25.

II. ANALYSIS

On appeal, Kidane challenges both grounds the district court used for dismissal. Each challenge triggers *de novo* review. *Simon v. Republic of Hungary*, 812 F.3d 127, 135 (D.C. Cir. 2016); *El Paso Nat. Gas Co. v. United States*, 750 F.3d 863, 874 (D.C. Cir. 2014). Unlike the district court, we do not reach the question whether the Wiretap Act authorizes a cause of action against Ethiopia for intercepting Kidane's communications. We instead conclude that the FSIA withdraws jurisdiction *in toto*.

The FSIA is "the 'sole basis for obtaining jurisdiction over a foreign state in our courts.'" *Weinstein v. Islamic*

Stevens, 529 U.S. 765 (2000). There, the High Court concluded that the statutory question was "logically antecedent" to Vermont's Eleventh Amendment immunity from suit and there existed "no realistic possibility" that answering the statutory question first "expand[ed] the Court's power beyond the limits that the jurisdictional restriction has imposed." *Id.* at 779 (internal quotation marks omitted).

[3] Ethiopia made several other arguments against the noncommercial-tort exception's applicability but the district court rejected each. *Doe*, 189 F. Supp. 3d at 17–18, 25–28. We need not address those arguments.

Republic of Iran, 831 F.3d 470, 478 (D.C. Cir. 2016) (quoting *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 434 (1989)). Unless an exception applies, "a foreign state shall be immune from the jurisdiction of the courts of the United States." 28 U.S.C. § 1604. One of those exceptions is the noncommercial-tort exception. It abrogates immunity from an action involving "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 or of any official or employee of that foreign state while acting within the scope of his office or employment[.]" *Id.* § 1605(a)(5).[4] The phrase "occurring in the United States" is no mere surplusage. "'[T]he entire tort'—including not only the injury but also the act precipitating that injury—must occur in the United States." *Jerez v. Republic of Cuba*, 775 F.3d 419, 424 (D.C. Cir. 2014) (quoting *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1525 (D.C. Cir. 1984)).

In *Jerez*, the plaintiff (Jerez) alleged he was intentionally injected with hepatitis C while imprisoned in Cuba. *See id.* at 421. He sued Cuba, relying on the noncommercial-tort exception. *Id.* at 424.[5] We found the exception inapplicable.

---

[4] Even in such circumstances, the FSIA restores sovereign immunity from suits "based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion [has been] abused" and from suits "arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights[.]" 28 U.S.C. § 1605(a)(5)(A)–(B).

[5] Jerez initially sued Cuba in Florida state court, where he obtained a default judgment. *Jerez*, 775 F.3d at 421. His case came to us through his efforts to execute the judgment on certain intellectual property. *Id.*

As we explained, the alleged injection of hepatitis C occurred abroad and we rejected Jerez's argument that a separate tort occurred each time the virus replicated in his body. *Id.* Replication showed only that Jerez suffered an "ongoing injury," not that the tort's precipitating act also occurred in the United States. *Id.* (emphasis omitted). To support his replication theory, Jerez "analogiz[ed] the defendants' actions to a foreign agent's delivery into the United States of an anthrax package or a bomb." *Id.* That analogy was flawed, we explained, because "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.*

Kidane argues that Ethiopia's tort is akin to the anthrax hypothetical. But the hypothetical was dictum and, of course, "[b]inding circuit law comes only from the holdings of a prior panel, not from its dicta." *Gersman v. Grp. Health Ass'n*, 975 F.2d 886, 897 (D.C. Cir. 1992). And *Jerez*'s holding hardly helps Kidane. *Jerez* squarely held that "the *entire* tort . . . must occur in the United States" for the noncommercial-tort exception to apply. 775 F.3d at 424 (emphasis added) (internal quotation marks omitted). Here, at least a portion of Ethiopia's alleged tort occurred abroad.

Maryland's intrusion-upon-seclusion tort shows why that is so. The tort covers "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, [making the intruder] subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Bailer v. Erie Ins. Exch.*, 687 A.2d 1375, 1380–81 (Md. 1997) (emphasis and internal quotation marks omitted) (quoting RESTATEMENT (SECOND) OF TORTS § 652B (1977)). There is thus no tort without intentional intrusion. But whether in London, Ethiopia or elsewhere, the tortious

intent aimed at Kidane plainly lay abroad and the tortious acts of computer programming likewise occurred abroad. Moreover, Ethiopia's placement of the FinSpy virus on Kidane's computer, although completed in the United States when Kidane opened the infected e-mail attachment, began outside the United States. It thus cannot be said that the entire tort occurred in the United States.

The two cases on which Kidane relies—*Liu v. Republic of China*, 892 F.2d 1419 (9th Cir. 1989), and *Letelier v. Republic of Chile*, 488 F. Supp. 665 (D.D.C. 1980)—are easily distinguished. In *Liu*, two gunmen allegedly acting at a Taiwanese admiral's direction assassinated a man in California, 892 F.2d at 1421; in *Letelier*, Chilean government agents allegedly constructed, planted and detonated a car bomb in Washington, D.C., 488 F. Supp. at 665. In both, the courts determined they had jurisdiction under the FSIA's noncommercial-tort exception to hear the victims' survivors' claims against the respective foreign sovereigns. *Liu*, 892 F.2d at 1425–26, 1431; *Letelier*, 488 F. Supp. at 673–74. Both involved actions "occurring in the United States" that were—without reference to any action undertaken abroad—tortious.

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. Kidane's Wiretap Act claim is similarly deficient. The Wiretap Act in pertinent part proscribes "intentional[] intercept[ions]" of "wire, oral, or electronic communication[s]." 18 U.S.C. § 2511(1)(a). But, again, the "intent[]," *id.*, and FinSpy's initial deployment occurred outside the United States. The tort Kidane alleges thus did not occur "entire[ly]" in the United States, *Jerez*, 775 F.3d at

424 (internal quotation marks omitted); it is a transnational tort over which we lack subject matter jurisdiction.

Kidane regards this conclusion as inconsistent with the noncommercial-tort exception's purpose and legislative history. He argues that, when the Congress codified the exception, it considered—but rejected—the approach of the European Convention on State Immunity. The European Convention abrogated sovereign immunity for certain torts if the facts underlying the torts occurred in the forum nation and if "the author of the injury or damage was present in that territory at the time." European Convention on State Immunity art. 11, *reprinted in Hearings on H.R. 11,315 Before the Subcomm. on Admin. Law & Governmental Relations of the H. Comm. on the Judiciary*, 94th Cong. 39 (1976) (1976 Hearings). Kidane notes the absence of similar language in section 1605(a)(5). We think Kidane reads too much into the Congress's silence.[6] As the Supreme Court has explained, the "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." *Amerada Hess Shipping Corp.*, 488 U.S. at 439–40. It is thus unsurprising that transnational cyberespionage should lie beyond section 1605(a)(5)'s reach.

Kidane also directs us to the FSIA's *commercial* activity exception to illuminate section 1605(a)(5)'s boundaries. The

[6] As the district court acknowledged, *Doe*, 189 F. Supp. 3d at 24, and as Ethiopia observes, when the State Department Legal Adviser was asked whether there was any inconsistency between the European Convention and the FSIA, he responded that—subject to one discrepancy not relevant here—there generally was not. 1976 Hearings, at 37.

commercial activity exception authorizes claims "based upon a commercial activity carried on in the United States by [a] foreign state[.]" 28 U.S.C. § 1605(a)(2). He observes that the Supreme Court, interpreting this provision, found instructive the "point of contact" between the tort and its victim in determining where the tort occurred. *OBB Personenverkehr AG v. Sachs*, 577 U.S. ____, 136 S. Ct. 390, 397 (2015) (internal quotation marks omitted). But *Sachs* underscores why the commercial activity exception is of limited usefulness here. There, the American plaintiff purchased a European rail travel pass from a Massachusetts travel agent. *Id.* at 393. When she used the pass to board the defendant Austrian state-owned railway's train in Innsbruck, Austria, she fell onto the tracks, where the moving train crushed her legs. *Id.* She sued, invoking the FSIA's commercial activity exception. *Id.* at 394. The Supreme Court concluded, however, that her lawsuit was not "based upon" the domestic sale of the rail pass. *Id.* at 393. It noted that "an action is based upon the particular conduct that constitutes the gravamen of the suit." *Id.* at 396 (internal quotation marks omitted). It explained that "the conduct constituting the gravamen of [her] suit plainly occurred abroad." *Id.*[7] But *Sachs* interpreted the commercial activity exception. And unlike the commercial activity exception, the noncommercial-tort exception does not ask where the "gravamen" occurred,

[7] In so concluding, the Court quoted a letter written by Justice Oliver Wendell Holmes to then-Professor Felix Frankfurter opining that "the 'essentials' of a personal injury narrative will be found at the 'point of contact'—'the place where the boy got his fingers pinched.'" *Sachs*, 136 S. Ct. at 397. Kidane reads *Sachs*—particularly its reliance on the "point of contact" language—as confirming that "a tort occurs at the place where the injury was inflicted upon the plaintiff." Appellant's Br. 14. We disagree with his reading.

id.; instead, it asks where the "*entire* tort" occurred, *Asociacion de Reclamantes*, 735 F.2d at 1525 (emphasis added).

For the foregoing reasons, we affirm the district court's dismissal of Kidane's intrusion-upon-seclusion claim for lack of subject matter jurisdiction. Because the same reasoning applies with equal force to Kidane's Wiretap Act claim, we affirm the dismissal of that claim as well.[8]

So ordered.

[8] We do not reach the applicability of the FSIA provisions governing discretionary functions or torts based upon misrepresentation or deceit. *See* 28 U.S.C. § 1605(a)(5)(A)–(B); *see also supra* n.4.

CERTIFICATE OF COMPLIANCE

I hereby certify that this petition has been prepared in 14-point Times New Roman, a proportionally spaced font, and does not exceed 3,900 words, excluding material not counted under Rule 32.

Dated: April 13, 2017

/s/ *Samuel L. Walling*
Counsel for Appellant

CERTIFICATE OF FILING AND SERVICE

I hereby certify that on this 13th day of April, 2017, I caused the foregoing Petition to be filed electronically with the Clerk of this Court using the CM/ECF System, which will send notice of such filing to the following registered CM/ECF users listed below. In addition, an original and 19 paper copies of this Petition will be filed with the Clerk of this Court.

/s/ *Samuel L. Walling*
Counsel for Appellant

ROBERT PHILLIP CHARROW
LAURA METCOFF KLAUS
Greenberg Traurig, LLP
2101 L Street, NW
Suite 1000
Washington, DC 20036

Counsel for defendant-appellee
Federal Democratic Republic of Ethiopia

DAVID A. KAYE
University of California School of Law
401 East Peltason Drive
Suite 1000
Irvine, CA 92697-8000

Counsel for amici curiae
United Nations Human Rights Experts