ORAL ARGUMENT SCHEDULED FOR FEBRUARY 2, 2017

United States Court of Appeals
For the District of Columbia Circuit

No. 16-7081

John Doe, a.k.a. Kidane,

Plaintiff/Appellant

v.

Federal Democratic Republic of Ethiopia,

Defendants/Appellees

Appeal from the United States District Court for the District of Columbia Case No. 1:14–cv-00372, Judge Randolph D. Moss

FINAL OPENING BRIEF FOR APPELLANT JOHN DOE

NATHAN CARDOZO CINDY COHN ELECTRONIC FRONTIER FOUNDATION 815 Eddy Street San Francisco, CA 94109 Tel. (415) 436–9333	RICHARD M. MARTINEZ SAMUEL L. WALLING ROBINS KAPLAN LLP 800 LaSalle Avenue, Ste. 2800 Minneapolis, MN 55402–2015 Tel.: (612) 349–8500

Counsel for Plaintiff-Appellant John Doe

December 27, 2016

SCOTT A. GILMORE
GUERNICA 37 INT'L JUSTICE CHAMBERS
Premier House, 3rd Floor
12-13 Hatton Garden
London, U.K EC1N 8AN
Tel.: +1 (510) 374-9872

Counsel for Plaintiff-Appellant John Doe

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

I. All Parties, Intervenors, and Amicis

A. Parties

1. Plaintiff

- John Doe, also known as Kidane

2. Defendant

- Federal Democratic Republic of Ethiopia

II. Ruling Under Review

The ruling under review is as follows:

- *Doe v. Fed. Democratic Republic of Ethiopia*, No. 1:14-cv-00372, 2016 U.S. Dist. LEXIS 67909 (D.D.C. May 24, 2016)

III. Related Cases

None.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

---

* Authorities upon which we chiefly rely are marked with asterisks.

Statutes

Rules

Other Authorities

JURISDICTIONAL STATEMENT

This is an appeal from a final order of the United States District Court for the District of Columbia. The action before the district court was for civil damages based on Defendant's tortious conduct, including for intrusion upon seclusion under Maryland common law and for violations of the Wiretap Act, 18 U.S.C. § 2510 *et seq*. The district court's subject matter jurisdiction is fully discussed *infra*.

The district court order dismissing Plaintiff's case as barred by the Foreign Sovereign Immunities Act ("FSIA"), 28 U.S.C. §§ 1602-1611, was entered on May 24, 2016. The notice of appeal was timely filed on June 22, 2016. This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes are contained in the addendum.

ISSUES PRESENTED

1) **Foreign Sovereign Immunity.** The FSIA non-commercial tort exception, 28 U.S.C. § 1605(a)(5), withdraws foreign sovereign immunity for torts occurring in the United States. Using spyware it installed on an American citizen's home computer in Maryland, Ethiopia intercepted and recorded his domestic communications

and activities—the gravamen of the wiretapping and privacy claims asserted below. Did these torts occur in the United States such that the non-commercial tort exception applies?

2) **Entity liability.** The Wiretap Act imposes criminal penalties on any "person" who unlawfully intercepts an electronic communication, 18 U.S.C. § 2511(1)(a), and civil liability on the "person or entity" that engaged in that violation, § 2520(a). Under basic agency principles, an entity can only act through its agents, and here Ethiopia's agents intercepted communications in violation of § 2511. Can Ethiopia be sued as an "entity" under § 2520 for its agents' violation of § 2511?

STATEMENT OF THE CASE

This case is about a foreign state that used sophisticated computer spyware to wiretap an American citizen's home computer in Maryland. Although the case involves a foreign sovereign and a technologically advanced scheme, the essential facts for purposes of this appeal are: (1) the citizen's communications were intercepted in the United States; and (2) the citizen's privacy was intruded upon in the United States.

Appellant, Mr. Kidane alleges that Appellee, the Federal Democratic Republic of Ethiopia ("Appellee" or "Ethiopia"), violated the Wiretap Act by intentionally intercepting his Skype telephone calls, made from his family computer in his home in Maryland.[1] Mr. Kidane further alleges that Ethiopia intentionally monitored his Web browsing and e-mail usage on his home computer, as well as that of his family, thereby intruding upon his seclusion.[2]

Ethiopia used state-of-the-art software called FinSpy to intercept Mr. Kidane's calls and to monitor Mr. Kidane's online activities, presumably because of Mr. Kidane's role in providing administrative and technical

[1] *See* Deferred Joint Appendix ("JA") at JA450-51.
[2] JA451.

support for a number of Ethiopian expatriates who raise awareness and advocate against the human rights abuses of the Ethiopian government. FinSpy is a commercial product designed for — and sold exclusively to — governments.[3] FinSpy attacks a target by first being included in an unassuming email attachment, thereby tricking the target into installing the FinSpy application on their computer. Once installed, the FinSpy application communicates with the government-customer's remote command and control server, which then automatically activates the application's eavesdropping capabilities.[4]

In this case, Ethiopia compromised Mr. Kidane's computer when he opened a Microsoft Word document that an acquaintance had e-mailed to him.[5] The document included hidden code for downloading and installing the FinSpy application on Mr. Kidane's computer. In addition, hard-coded within the document was the Internet Protocol address, or "IP address" of the command-and-control server.[6] That server, which later received the information that the FinSpy application on Mr. Kidane's computer

[3] JA431, JA436-43, JA453-58.
[4] *Id*.
[5] JA431, JA443, JA473-75.
[6] JA440, JA444, JA447.

intercepted, was located in Ethiopia, on a block of IP addresses owned by the official state-run telecommunications company of Ethiopia, and controlled by the Appellee.[7]

Ethiopia activated the FinSpy application on Mr. Kidane's computer on October 31, 2012, and kept the application active until March 18, 2013.[8] During this time, Ethiopia's FinSpy software application secretly recorded dozens (and perhaps hundreds) of Mr. Kidane's Skype Internet phone calls.[9] In addition, the software monitored and recorded Mr. Kidane's Web browsing history, his social network activity and e-mail usage.[10] Because the computer was shared by his family, the FinSpy application intercepted everything done by the family on the computer – from private correspondence to research his children conducted for their schoolwork. The family was subjected to this unfettered surveillance for nearly five months.

Ethiopia sought to cover up its eavesdropping activities after it was caught red-handed and publicly exposed by The Citizen Lab, at the

---

[7] JA444.
[8] JA447-48.
[9] JA445-46.
[10] JA446-47.

University of Toronto's Munk School of Global Affairs, for operating a FinSpy command-and-control server — the same server, with the same hard-coded IP address found in the document that infected Mr. Kidane's computer. Following publication of the Citizen Lab report, Ethiopia attempted to erase from Mr. Kidane's computer the evidence of FinSpy's activities.[11] Due to a technical failure, however, the attempt failed, and Mr. Kidane was able to discover the intrusion after the fact.[12]

Mr. Kidane filed this lawsuit on February 13, 2014 in the United States District Court for the District of Columbia, alleging violations of the Wiretap Act under federal law, and intrusion upon seclusion under Maryland common law. Ethiopia moved to dismiss the Complaint on June 27, 2014, and Mr. Kidane filed a First Amended Complaint on July 18, 2014. Ethiopia moved to dismiss the First Amended Complaint on August 4, 2014. Of relevance here, Ethiopia argued that (1) the Foreign Sovereign Immunities Act ("FSIA") barred the asserted claims, and (2) the Wiretap Act did not create a cause of action against foreign states. In a May 24, 2016 Memorandum and Opinion (amended on August 2, 2016 to correct a single

[11] JA442, JA444-46, JA459-72.
[12] *Id.*

typographical error), the district court granted Ethiopia's motion. Mr. Kidane now challenges those rulings in this appeal.

SUMMARY OF THE ARGUMENT

The district court's dismissal of Mr. Kidane's complaint was legal error. By intercepting Mr. Kidane's private communications entirely within the state of Maryland, Ethiopia subjected itself to liability for violation of the Wiretap Act and for the Maryland common law tort of intrusion upon seclusion. Under this Court's precedent in *Jerez*, the injury *and* the precipitating acts causing Mr. Kidane's injury took place in the United States, thereby satisfying the "entire tort" rule. Furthermore, consistent with Congress's modifications to the Wiretap Act to add liability for "entit[ies]," Ethiopia is subject to liability under the Wiretap Act as a government "entity". Ethiopia's acts subjecting it to liability do not call for the exercise of any political judgment, and do not raise any political questions.

While the district court repeatedly acknowledged that the issues raised by Mr. Kidane's case were "close" questions, its decision to ultimately dismiss the complaint was made in error. For the reasons more fully explained below, Mr. Kidane respectfully requests that this Court

reverse the district court's decision and remand the case for further proceedings.

ARGUMENT

Issue One – Foreign Sovereign Immunity

Standard of Review

When reviewing a district court's dismissal of a complaint under the FSIA, the Court reviews "de novo whether [the] facts are sufficient to divest the foreign sovereign of its immunity." *Nemariam v. Fed. Democratic Republic of Ethiopia*, 491 F.3d 470, 475 (D.C. Cir. 2007). The Court must "take the [appellant's] factual allegations as true and determine whether they bring the case within any of the exceptions to immunity invoked by the [appellant]." *Id.* (citation omitted).

I. Ethiopia waived its immunity under the FSIA non-commercial tort exception because it wiretapped, monitored, and intercepted Mr. Kidane's communications at his home in Maryland.

The central question in this case is whether the FSIA permits foreign states to evade liability for committing certain torts within the United States by using advanced technology to violate the law rather than traditional human agents. Here, a foreign state used an e-mail attachment to install sophisticated computer software, programmed to intercept and

record private communications, on an American citizen's home computer in Maryland. If a foreign state's agents had personally executed these acts by, for example, physically placing a recording device in an American citizen's home or on an American citizen's telephone line, there would be no doubt that the FSIA would not shield the state from civil liability. Yet the foreign state here claims immunity from U.S. courts because modern technology gives it the means to invade Americans' homes, to listen into their conversations, and to violate their privacy without its human agents ever setting foot on American soil. But advances in technology do not provide license to foreign states to conduct an end-run on the FSIA, and to wiretap Americans in their homes with impunity.

The FSIA, 28 U.S.C. §§ 1330, 1602–1611, is the sole basis for jurisdiction over foreign states. *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 439 (1989). The FSIA replaced the previous system where courts had to decide, individually, whether immunity applied in a particular case, and instead vests subject matter jurisdiction whenever a claim falls within one of the statutory exceptions to immunity. *Id.*

At issue here, the FSIA's non-commercial tort exception waives immunity in claims 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."[13] 28 U.S.C. § 1605(a)(5). The FSIA ensures that, where an exception applies, a foreign state will be liable "in the same manner and to the same extent as a private individual under like circumstances." 28 U.S.C. § 1606.

Here, the non-commercial tort exception permits Mr. Kidane's claims for wiretapping under 18 U.S.C. §§ 2511(1)(a), 2520; and for intrusion upon seclusion under Maryland common law. Because Ethiopia's immunity is central to this case and dispositive of these claims, this Court should resolve the FSIA issue first. The district court erred by first addressing the merits issue of whether Mr. Kidane states an actionable claim under the Wiretap Act, because "resolving a merits issue while jurisdiction is in doubt 'carries the courts beyond the bounds of authorized judicial action.'" *In re Papandreou*, 139 F.3d 247, 254-55 (D.C. Cir. 1998) (quoting *Steel Co. v.*

[13] The tort exception bars claims arising from discretionary acts, and those based on certain enumerated torts (malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights). 28 U.S.C. 1605(a)(5)(A) and (B). The district court correctly held that none of these exclusions bar Mr. Kidane's claims against Ethiopia. JA681-83 (enumerated torts), JA695-701 (discretionary acts).

Citizens for a Better Environment, 523 U.S. 83, 94 (1998)). Nevertheless, as discussed below, that substantive ruling was also in error.

A. The asserted torts occurred in the United States under the "entire tort" rule because Ethiopia's spyware intercepted Mr. Kidane's communications and intruded upon Mr. Kidane's seclusion at his home in Maryland.

This Court has held that for the non-commercial tort exception to apply, the "entire tort" must occur in the United States." *Associacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1525 (D.C. Cir. 1984).[14] This Court has further held that an "entire tort" has two components: (1) the injury and (2) the act precipitating that injury. *See Jerez v. Republic of Cuba*, 775 F.3d 419, 424 (D.C. Cir. 2014) (interpreting *Amerada Hess,* 488 U.S. at 441). Since there is no dispute that Mr. Kidane's injuries occurred in the

[14] The Court is joined by the Second, Sixth, and Ninth Circuits in adopting the "entire tort" rule. *See*, *e.g.*, *O'Bryan v. Holy See,* 556 F.3d 361, 382 (6th Cir. 2009) (recognizing entire tort rule under *Amerada Hess*); *Cabiri v. Government of Ghana,* 165 F.3d 193 (2d Cir. 1999) (same); *Olsen v. Gov't of Mexico*, 729 F.2d 641, 646 (9th Cir. 1984). But the Supreme Court has never adopted the "entire tort" terminology. Nor did *Amerada Hess* cite *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1525 (D.C. Cir. 1984), or any other case adopting the "entire tort" rule. Because *Amerada Hess* only stands for the limited proposition that an extraterritorial tort with domestic effects falls outside the tort exception, Appellant does not concede that *Amerada Hess* requires applying the "entire tort" rule to the present case.

United States, the only question is whether the acts precipitating those injuries occurred in the United States.[15] They did.

1. The "entire tort" rule focuses on whether the defendants' infliction of injury on the plaintiff occurs entirely within the United States.

In *Jerez v. Republic of Cuba* this Court held that a means for determining where the precipitating acts occurred is by examining where the infliction of injury occurred. Under this Court's rule in *Jerez,* 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.*[16] Here, the infliction of injury was the interception and recording of Mr. Kidane's computer activities in Maryland. Thus, the acts precipitating Mr. Kidane's injuries occurred in the United States. Alternatively, the precipitating acts occurred in the United States because Ethiopia caused Mr. Kidane's injuries to occur in Maryland.

Jerez illustrates where an injury-precipitating act occurs by contrasting the facts of that case with a hypothetical case. In *Jerez*, the plaintiff was

---

[15] JA686.

[16] As explained below, Judge Moss's ruling incorrectly separates "infliction" from "injury," (Dkt. 39 at 27) thereby linking the location of the infliction of injury to the location of the injury only, rather than to the location of the acts that precipitated the injury as in *Jerez*. *Jerez*, 775 F.3d at 424.

imprisoned and tortured for many years in Cuba, where he was purposefully injected with the hepatitis C virus. *Jerez*, 775 F. 3d at 421. In the contrasting hypothetical, foreign agents use the mail to deliver "an anthrax package or bomb" "into the United States." *Id.* at 424.[17] In Jerez's case, the act that precipitated the injury—the injection (referred to as the infliction of injury)—occurred in Cuba. Only the "ongoing injury," the replication of the virus, occurred in the United States. But in the hypothetical anthrax case, the act that precipitated the injury—the exposure (also referred to as the infliction of injury) and the anthrax infection (the injury) occurred in the United States. *Id.* Thus, the latter satisfies the entire tort rule while the former did not. *Id.*

The *Jerez* rule's focus on where the infliction of injury occurred is squarely in line with the Supreme Court's analogous test for where a tort occurred under the FSIA commercial activities exception, as set forth in *OBB Personenverkehr AG v. Sachs*, 136 S. Ct. 390, 393-96 (2015). That case held that the sale of train tickets in the United States was not sufficient to

[17] *See also Jerez v. Republic of Cuba, et al.*, No. 2013-7141, Document No. 1490676 at 25 (D.C. Cir. 2014) (posing hypothetical in which a "package that was mailed from abroad . . . contained a chemical agent or biological weapon, for example anthrax.").

provide jurisdiction over a personal injury lawsuit against the Austrian Government arising from the train's crash in Austria because the gravamen of the claim occurred outside the United States. *Id.* In considering the question of precisely where the claimed tort occurred, the *Sachs* Court drew clarity from Justice Holmes, who wrote 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." Letter (Dec. 19, 1915), in *Holmes and Frankfurter: Their Correspondence, 1912–1934*, p. 40 (R. Mennel & C. Compston eds. 1996) (cited in *Sachs*, 136 S.Ct. at 397). And so *Sachs*, like *Jerez*, supports the proposition that a tort occurs at the place where the injury was inflicted upon the plaintiff.

2. The "entire tort" rule is satisfied here because Ethiopia inflicted injury on Mr. Kidane in Maryland.

Ethiopia inflicted injury on Mr. Kidane when its spyware, resident and running on the Kidane family computer, intercepted Mr. Kidane's communications and recorded Mr. Kidane's computer activities. It was these acts in Maryland, and these acts alone, that violated the Wiretap Act and invaded Mr. Kidane's privacy. Thus, both the injury and the act precipitating that injury occurred in the territorial United States.

As alleged in the First Amended Complaint, Ethiopia's spyware—the FinSpy software module—was installed and ran on Mr. Kidane's home computer in Maryland.[18] Once installed, the FinSpy software module running on Mr. Kidane's computer in Maryland digitally intercepted and recorded his Skype Internet phone calls, and monitored and recorded his and his family's web browsing history and email usage.[19] The torts were complete—and these causes of action accrued—the moment FinSpy's recordings and monitoring logs were stored locally on Mr. Kidane's computer in Maryland.[20]

That the acts precipitating Mr. Kidane's claimed injuries occurred in the U.S. is buttressed by the fact that, following installation and activation, Ethiopia's spyware performed the illegal surveillance on Mr. Kidane's computer *automatically*, "without intervention of the Ethiopian master server."[21] Ethiopia's agents did not manually trigger each interception or recording from their computer terminals in Ethiopia.[22] Instead, the FinSpy module in Maryland was programmed to automatically record the

---

[18] JA430-31.
[19] JA430-31.
[20] JA430-31.
[21] JA445.
[22] JA445.

incoming and outgoing audio streams of all of Mr. Kidane's Skype calls, all of which were made from Maryland.[23]

Similarly, the FinSpy module in Maryland automatically monitored and created records concerning Mr. Kidane's e-mailing and web browsing in Maryland. Thus, the intercepting and recording, the acts that precipitated Mr. Kidane's injuries, like the hypothetical opening of the envelope and anthrax infection in *Jerez*, occurred entirely in the United States, without contemporaneous direction from any human actor in Ethiopia, or the presence of any human actor in the United States.

These allegations are sufficient to demonstrate that, for both the Wiretap Act claim and the intrusion upon seclusion claim, Ethiopia's infliction of injury on Mr. Kidane occurred entirely in Maryland. As soon as the interception occurred and the recordings were made, the damage was done to Mr. Kidane's privacy, and the torts of wiretapping and intrusion upon seclusion were complete.

The district court erred in stating that "all of the acts by Ethiopia or its agents that allegedly precipitated the tort occurred outside the United

[23] JA445.

States."[24] This statement is erroneous because it considers only the acts of flesh-and-blood individuals, and ignores the acts carried out by technological devices at the behest of those individuals.

The law has long held that individuals can act through tools or devices. Indeed, the idea that people can act through technological devices is embedded in the Wiretap Act itself. The Wiretap Act prohibits individuals from, *inter alia*, intercepting electronic communications. 18 U.S.C. § 2511(1)(a). Obviously, a human being cannot directly intercept an electronic communication. § 2510(12) (defining "electronic communication"). Rather, the individual must employ a technological device, which performs the acts of intercepting the communication, and then rendering the communication in a format that is understandable to humans. As a result, the Act defines an interception as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of *any electronic, mechanical, or other device*." 18 U.S.C. § 2510(4) (emphasis added). Thus, in a literal sense, the Wiretap Act focuses on the act performed by the technological device, and imputes that act to the individual that controls the technological device.

[24] JA686, JA688.

Here, Ethiopia acted through the FinSpy module that was installed on Mr. Kidane's computer and activated by Ethiopia's server. The FinSpy module is the "electronic, mechanical or other device" that performed the act of intercepting Mr. Kidane's electronic communications in the United States. This act must be imputed to Ethiopia. As a result, it is factually incorrect—and clear error—to assert that "*all* of the acts by Ethiopia or its agents that allegedly precipitated the tort occurred outside the United States."[25] The FinSpy module, operating in the United States, was Ethiopia's agent, just as a human spy would have been.

3. The tortious acts occurred in Maryland as the causes of action for the asserted torts accrued entirely in Maryland.

While the *Jerez* rule is precedent in this Circuit, its conclusion is buttressed by consideration of whether the individual causes of action for the claimed torts accrued in the United States. They did.

As previously discussed, Mr. Kidane asserts violations of the Wiretap Act under federal law, and intrusion upon seclusion under Maryland common law. The Wiretap Act is straightforward. It assigns liability to "any person who . . . intentionally intercepts, endeavors to intercept, or

[25] JA686, JA688 (emphasis added).

procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). Similarly, Maryland common law holds that "the gravamen" of the tort of intrusion upon seclusion "is the intrusion into a private place or the invasion of a private seclusion that the plaintiff has thrown about his person or affairs." *New Summit Assocs. Ltd. P'ship v. Nistle*, 533 A.2d 1350, 1354 (Md. Ct. Spec. App. 1987). As the district court noted, under Maryland common law, a plaintiff "need not allege that a *physical* trespass occurred to state a claim for intrusion upon seclusion."[26]

As applied to the present circumstances, both of the torts were completed—and the causes of action underlying this case accrued—in Maryland when FinSpy intentionally intercepted and recorded Mr. Kidane's electronic communications.

a. Defendant Violated the Wiretap Act in Maryland.

The Wiretap Act does not have extraterritorial effect. Thus, to succeed, a claimed Wiretap Act violation ***must*** occur within the United States. Given this jurisdictional limitation, a finding that a set of facts involves a domestic

[26] JA687 (citing See Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir. 1969) (emphasis added).

application of the Wiretap Act necessarily leads to the conclusion that the claimed violation satisfies the "entire tort" rule, as expressed in *Jerez*.

Every court that has examined the extraterritoriality of the Wiretap Act has held that the site of interception determines whether the Wiretap Act is being applied domestically or extraterritorially. The Wiretap Act defines an interception as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of *any electronic, mechanical, or other device*." 18 U.S.C. § 2510(4) (emphasis added). Under federal law, "the recording of a telephone conversation alone 'constitutes an 'aural . . . acquisition' of that conversation" under the Wiretap Act. *See Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir. 1994).

In *United States v. Glover*, a D.C. federal judge authorized placing a wiretap in a truck located in Maryland, while officers could hear the calls from a listening post in D.C. 736 F.3d 509, 515 (D.C. Cir. 2013). However, as this Court recognized, a district court only has jurisdiction to issue a warrant under the Wiretap Act, 18 U.S.C. § 2518(3), and Rule 41(b)(1) of the Federal Rules of Criminal Procedure, "if the person or property [to be searched] is located within the district" of the issuing court. *Id.* at 514.

This Court held that jurisdiction lies at the site of interception, *i.e.*, "the property on which the device is . . . installed." *Id*. *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 *Glover* panel expressly rejected the "listening post" argument, which tied jurisdiction to the place where agents listened to intercepted communications, instead ruling that the site of interception—the location of the precipitating act in *Jerez*'s framing—determines the basis for jurisdiction in a Wiretap Act case. *Id.*

Additional, similar examples abound. For example, in *Huff v. Spaw*, the Sixth Circuit considered the allegation that an individual in Kentucky used an iPhone to record a phone conversation that originated from a mobile phone in Italy, and held that the allegation involved a domestic application of the Wiretap Act because the interception occurred in the United States. 794 F.3d 543, 547 (6th Cir. 2015); *see also United States v. Cotroni*, 527 F.2d 708, 711 (2d Cir. 1975) ("[I]t is not the route followed by foreign communications which determines the application of Title III; it is where the interception took place."); *cf. United States v. Peterson*, 812 F.2d 486, 492 (9th Cir. 1987) (holding Wiretap Act does not apply

extraterritorially to radio transmissions intercepted in Philippines); *United States v. Tirinkian*, 502 F. Supp. 620, 627 (D.N.D. 1980), *affd. United States v. Wentz*, 686 F.2d 653 (8th Cir. 1982) (the law of the point of interception governs the legality of the surveillance).

Here, precedent establishes that because the place of interception was in the United States, Ethiopia violated the Wiretap Act domestically. That ends the "entire tort" inquiry under *Jerez*. Since the Wiretap Act is not extraterritorial, *Cotroni*, 527 F.2d at 711, a well-pleaded wiretap claim based upon a domestic interception is *ipso facto* an "entire tort" occurring in the United States.

b. The intrusion upon seclusion also occurred in Maryland.

Just as the Wiretap Act was violated in Maryland, the same must be said for Defendant's intrusion upon seclusion. Under Maryland common law, the focus of this tort is the "intrusion into a private place." *New Summit Assocs. Ltd. P'ship v. Nistle*, 533 A.2d 1350, 1354 (Md. App. 1987). That private place was in Mr. Kidane's home and his home computer. In this case, just as in *Glover*, the wiretapping occurred in Maryland at the site of interception. Thus, the "entire tort" occurred in Maryland.

For both alleged torts the precipitating acts and the injury all occurred on U.S. soil. Consequently, the entirety of the alleged torts occurred in Maryland, and the non-commercial tort exception to immunity applies.[27]

B. The district court erred in adopting Ethiopia's view of the facts and concluding that the acts precipitating the alleged torts occurred outside the territorial United States.

The district court's order hinges on the erroneous decision to adopt Ethiopia's theory of where the alleged torts occurred.[28] The district court correctly acknowledged that, under *Jerez*, both the injury and the acts precipitating the injury must occur in the United States. Still, despite conceding that Ethiopia's "argument is incomplete because it fails to grapple with the modern world in which the Internet breaks down traditional conceptions of physical presence" the district court incorrectly

---

[27] Further, no court has ever held that the "entire tort" rule requires identifying the *locus* of every element of every claim, an approach that would be totally incompatible with the Supreme Court's analysis in *Amerada Hess* and this Court's in *Jerez*, neither of which undertook such an exhaustive element-by-element analysis of the respective causes of action. "[N]or did [they] engage in the choice-of-law analysis that would have been a necessary prelude to such an undertaking." *OBB Personenverkehr AG v. Sachs*, 136 S. Ct. 390, 396 (2015) (discussing analogous issues under § 1605(a)(2) and holding that engaging in an element-by element analysis would "require a court to identify all the elements of each claim in a complaint before that court may reject those claims for falling outside [§ 1605(a)(5)].").

[28] JA688.

held that "all of the acts by Ethiopia or its agents that allegedly precipitated the tort occurred outside the United States."[29] The court thereby incorrectly shifted the focus from what Ethiopia's FinSpy software agent did in Maryland to what Ethiopia's flesh-and-blood agents did in Ethiopia.[30]

This critical error fuels each "reason" that the district court puts forth in support of its decision.[31] As explained below, the underlying factual determination, and the conclusions that the district court draws from it, are incorrect.

1. The district court first erred in accepting Ethiopia's improperly expansive view of what acts precipitated the injury.

Ethiopia's argument focused on its preparatory acts, including its control of the FinSpy, the formation of intent, the drafting of the e-mail that delivered the FinSpy, etc., all of which occurred in Ethiopia. The district court erred by failing to recognize the distinction between these preparatory, non-tortious, acts that occurred before the infliction of the injuries and the acts that actually precipitated (or inflicted) the injuries. Precedent makes the importance of this distinction clear.

---

[29] JA686, JA688.
[30] JA688.
[31] JA688-95.

First, in the landmark tort-exception case *Letelier v. Republic of Chile*, the assassination of a former Chilean diplomat in Washington DC was orchestrated entirely from within Chile. 488 F. Supp. 665, 673 (D.D.C. 1980) (cited with approval in *MacArthur Area Citizens Ass'n v. Republic of Peru*, 809 F.2d 918, 922 n.4 (D.C. Cir. 1987)). This Court nonetheless allowed the case to proceed against the defendant Republic of Chile under section 1605(a)(5), even though the Chilean officials who planned and ordered the assassination were not physically present in the United States.

Also, in *Liu v. Republic of China*, an official of the Republic of China coordinated a contract killing in California. 892 F.2d 1419, 1434 (9th Cir. 1989). The official did not enter the United States himself, but hired and trained gang members to execute the killing. *Id.* at 1423-24. Again, the fact that the Chinese official was not physically present in the United States did not prevent the court from holding that the claims could proceed against the defendant Republic of China under section 1605(a)(5). *Id.* at 1425. Having determined that FSIA conferred jurisdiction on the court to hear the case, the court went on to cite *Letelier* in holding that the act of state doctrine did not mandate abstention. *Id.* at 1432.

The facts of this case are similar to those in *Letelier* and *Liu*. In those two cases, this Court and the Ninth Circuit recognized that the planning and preparations occurred outside of the United States, but the infliction of injuries and the injuries themselves occurred within the United States. The same is true here. Therefore, the district court's conclusion cannot be correct.

The district court's statement that "the question of where the 'entire tort' occurred cannot be wholly divorced from the physical location of the tortfeasors"[32] incorrectly implies that there is a "physical presence" requirement embedded within the non-commercial tort exception. Such a proposition stands in direct contradiction to *Letelier and Liu* where the courts held that the non-commercial tort exception applies despite the fact that the foreign officials who orchestrated the intentional torts were not physically present in the United States. Foreign governments can be held liable for setting into motion torts that are consummated in the United States, without ever being physically present in the United States.

Letelier and *Liu* also refute the district court's statement that "Kidane, moreover, fails to identify any case applying the non-commercial tort

[32] JA688.

exception to circumstances, like those alleged here, where the precipitating acts of the relevant tortfeasor occurred outside the United States."[33] Under Ethiopia's (and the district court's) incorrect definition, the precipitating acts in both *Liu* and *Letelier* occurred in the Republic of China and the Republic of Chile, respectively. That is where the intent, planning, and direction occurred.[34] Even so, the cases were allowed to go forward.

2. The district court erred again in limiting the *Jerez* "infliction of injury" analysis to determining where the claimed injury occurred.

This Court's decision in *Jerez* did not tie the location of infliction of injury to the location of the claimed injury. Rather, the *Jerez* Court began by observing that Jerez had claimed an "ongoing *injury* that he suffers in the United States." The Court noted that "not only the injury, but also the act precipitating the injury—must occur in the United States." 775 F.3d at 424. The *Jerez* Court then held that the "infliction of injury on Jerez occurred entirely in Cuba," meaning that the acts precipitating Jerez's injury occurred in Cuba. *Id*. Thus, the entire tort did not occur in the United States and Jerez's claim was barred.

---

[33] JA689.
[34] JA686. Both cases were cited by the Appellant below.

The *Jerez* Court also considered Jerez's hypothetical tort, in which foreign agents deliver an anthrax package or bomb into the United States. *Id*. The Court determined that the hypothetical claim would succeed because the infliction of the injury (exposure to anthrax) would occur in the United States.

The *Jerez* Court's analysis demonstrates that infliction or injury relates to the locus of the acts precipitating the injury, not the locus of the injury itself. That interpretation is supported by the plain meaning of "inflict" and "precipitate," which both mean to cause or bring about.[35] Hence, to say that the infliction of injury occurs in a place is to say that the acts precipitating the injury occur in that place.

In dismissing this Court's analysis in *Jerez*, the district court disregarded the *best* precedent available concerning how the controlling question in this case should be resolved. The FinSpy module on Mr. Kidane's computer is directly analogous to the hypothetical anthrax package mailed into the United States—both involved activity and preparation outside of the United States, both were delivered from outside the United States, and both inflicted injury in the United States. In stating

[35] *Merriam-Webster's Collegiate Dictionary* 641, 977 (11th ed. 2012).

that the latter would satisfy the "entire tort" rule, the *Jerez* court explained that the precipitating acts are not the unbounded preparatory acts that precede an injury, they are the specific acts that inflict the injury. *Jerez*, 775 F. 3d at 424. Thus, although this case involves some preparatory activity in Ethiopia, the acts that inflicted injury—the interception and monitoring of Mr. Kidane's communications—occurred in the United States and the "entire tort" rule is satisfied here as well.

A simple hypothetical illustrates the type of wiretapping that would run afoul of *Amerada Hess* and *Jerez*, and fall outside the non -commercial tort exception. Suppose Mr. Kidane had placed a Skype call from his computer in Maryland to a friend in Ethiopia. And suppose Ethiopia used FinSpy installed on the friend's computer in Ethiopia to record the conversation. In that scenario, the injury to Mr. Kidane's privacy would have occurred in the United States. But the interception that precipitated that injury would have taken place overseas, in Ethiopia where the FinSpy module was engaged. That is precisely what *Amerada Hess* precludes: an overseas tort causing "direct effects in the United States." 488 U.S. at 441. But that is not what happened here. Thus, the district court conflated the

extraterritorial wiretapping of a domestic victim with the domestic wiretapping of a domestic victim.

Unlike the rulings in *Amerada Hess* and *Jerez*, the district court's error results not just in a choice of jurisdiction; it effectively eliminates any jurisdiction for these torts. Since Mr. Kidane's communications were not intercepted in Ethiopia, there is likely no jurisdiction there either. If, as the lower court found, these torts did not occur in the United States, then they did not occur anywhere, meaning that Ethiopia, or any other government that engages in this sort of attack on American citizens in the United states, can do so with impunity.

C. The district court erred in finding that this case raised political questions, even after the Executive Branch declined to intervene.

The district court also erred in finding that applying the noncommercial tort exception to this case "involves a political judgment, raising sensitive issues of foreign relations." JA693. This is wrong for three reasons.

First, it rests on the flawed premise that the "torts [were] precipitated exclusively beyond the borders of the United States . . . ." *Id.* As shown above, Mr. Kidane's personal injuries were precipitated by FinSpy's

interception and recording activities in Maryland. Thus, this case simply does not raise the issue of a U.S. court passing judgment on the acts of a foreign state taken within its own territory. Mr. Kidane does not seek review of Ethiopia's domestic wiretapping program—only of its surveillance activities in U.S. territory that were in violation of U.S. law.

Second, this case does not "turn on standards that defy judicial application." *Baker v. Carr*, 369 U.S. 186, 211 (1962). The Supreme Court has held that the "interpretation of the FSIA's reach" is a "pure question of statutory construction . . . well within the province of the Judiciary." *Republic of Austria v. Altmann*, 541 U.S. 677, 701 (2004). And this case hinges on statutory construction. Mr. Kidane asserts a violation of statutory and common law rights under the FSIA, a jurisdictional framework that was designed to "transfer primary responsibility for deciding 'claims of foreign states to immunity' from the State Department to the courts." *Samantar v. Yousuf*, 560 U.S. 305, 313 (2010) (quoting 28 U.S.C. § 1602). A central issue in this case—determining the *situs* of a Wiretap Act violation—is one which this Court and others have already addressed, not as a political judgment, but as a straightforward exercise in statutory construction. *See United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013).

The fact that the defendant is a foreign sovereign does not alter this settled *situs* analysis, or invite a political judgment, because, in enacting the FSIA, Congress made clear that "the foreign state shall be liable in the same manner and to the same extent as a private individual under like circumstances." 28 U.S.C. § 1606. Perhaps recognizing that this case entails no political judgment or "sensitive issues of foreign relations," the State Department declined to offer its views, despite the district court's invitation.[36] Thus the court was wrong to invoke political concerns that were never raised by the political branches.

Finally, the district court erred in finding that applying the non-commercial tort exception to computer hacking would require "adjust[ing] the rules of foreign sovereign immunity to new and unanticipated events that might arise." JA693. Mr. Kidane has asked the Court to apply the non-commercial tort exception—a statute intended to apply to "*all tort actions* for money damages," S. Rep. No. 94-1310, 20 (1976). Applying an older statute to new facts and circumstances is the essence of statutory interpretation and a core judicial function. As the Supreme Court noted, "the Judiciary has a responsibility to decide cases properly before it, even

[36] Notice by the United States, Sept. 25, 2015, JA664-65.

those it 'would gladly avoid.' *Zivotofsky ex rel. Zivotofsky v. Clinton*, 132 S. Ct. 1421, 1427 (2012) (quoting *Cohens v. Virginia*, 6 Wheat. 264, 404, 5 L.Ed. 257 (1821)).

D. The district court erred in impliedly holding that the text, history, or purpose of Section 1605(a)(5) requires the presence of a human tortfeasor in the jurisdiction of suit.

The district court found that the torts did not occur in the United States for one key reason: no tortfeasor was physically present on U.S. soil. *See* JA695. But the court could cite no textual basis for requiring the tortfeasor's presence: there was none to cite. On the contrary, the text, history, and purpose of the non-commercial tort exception indicate that it covers tort claims for injuries inflicted in the United States by a device owned and operated by a foreign sovereign.

1. The plain language of the FSIA does not require the presence of a human tortfeasor.

The words "physical presence of the tortfeasor" are nowhere found in the text of § 1605(a)(5). Indeed, the statute does not require a human tortfeasor at all. Section 1605(a)(5) withdraws immunity for injuries "caused by the tortious act or omission *of that foreign state* or of any official or employee of that foreign state." (emphasis added). The text

distinguishes between the act of a "foreign state" and that of its human "official or employee."

This distinction is not superfluous. A state can be liable for injuries inflicted by its human agents, but it can also be liable, "as a proprietor and user, for the evil caused by an inherently dangerously instrumentality." *Harbin v. D.C.*, 336 F.2d 950, 953 (D.C. Cir. 1964) (Washington, J., concurring) (holding that District of Columbia can be strictly liable for injuries caused by unmuzzled police dog). Congress was aware of liability in tort for animals and instrumentalities when it enacted the FSIA. *Cf. Astoria Fed. Sav. & Loan Assn. v. Solimino*, 501 U.S. 104, 108 (1991) ("Congress is understood to legislate against a background of common-law . . . principles."). In fact, the House Report states that that the tort exception was "meant to include causes of action which are based on strict liability." H. Rep. 94-1487 at 21. If Congress had intended to exclude such torts by requiring the presence of a human tortfeasor, it would have said so.

2. The district court misread the FSIA's legislative history to require the presence of the tortfeasor—a requirement Congress had studied and rejected.

The district court reasoned that the FSIA tort exception requires the physical presence of a human tortfeasor because Congress sought to mirror

the European Convention on State Immunities ("European Convention"), and that Convention specifically includes a presence requirement in its tort exception. JA695.

But the district court has it backwards. The fact that Congress studied the Convention, and knew it required the presence of a tortfeasor, only shows that Congress knowingly omitted that requirement from the FSIA.

Congress was well-familiar with the European Convention. It even reprinted a copy of the European Convention in the legislative record. Hearings on H.R. 11,315 Before the Subcomm. on Admin. Law & Gov't Relations of the H. Comm. on the Judiciary, 94th Cong. 29, 37 (1976) ("1976 Hearing"). Yet Congress pointedly did not choose to adopt the tort exception contained in the European Convention, which expressly requires that the author of the injury or damage be present in the territory at the time of the tort:

> A Contracting State cannot claim Immunity from the Jurisdiction of a court of another Contracting State in proceedings which relate to redress for injury to the person or damage to tangible property, if the facts which occasioned the injury or damage occurred in the territory of the State of the forum, and *if the author of the injury or damage was present in that territory* at the time when those facts occurred.

Article 11, European Convention, *reprinted in* 1976 Hearing at 39 (emphasis added).

If Congress had intended the FSIA to track the European Convention's tort exception word-for-word, it would have done so. Yet no such requirement is found in the early or final versions of the Act. *See* Pub. L. 94-583, 90 Stat. 2891 (1976); S. 771, 93d Cong. (1973); H.R. 3493, 93d Cong., 1st Sess. (Jan. 31, 1973). Thus Congress was fully aware of the territorial requirement in the European Convention and, perhaps realizing that this limitation would not sufficiently future-proof the statute, chose not to include it.

The district court erred in creating a new requirement for the non-commercial tort exception that was known to and specifically not included by Congress.[37] As the Supreme Court has observed: "[W]e should not take it upon ourselves to extend the waiver [of sovereign immunity] beyond

---

[37] The district court also cited reciprocity and comity as another reason for requiring the tortfeasor's presence on U.S. soil. But it did not actually survey foreign immunity laws to determine what comity might require. JA692-93. In fact, just like the FSIA, foreign state immunity laws in the key common-law countries do not expressly require the tortfeasor's presence. *See, e.g.*, State Immunity Act 1978, c. 33, sec. 5 (UK) (no reference to tortfeasor's presence in personal injury exception); State Immunity Act (R.S.C., 1985, c. S-18), sec. 6 (Canada) (same); Foreign State Immunities Act 1985, sec. 13 (Australia) (same).

that which Congress intended . . . . Neither, however, should we assume the authority to narrow the waiver that Congress intended." *U.S. v. Kubrick*, 444 U.S. 111, 117–118 (1979) (emphasis added) (referencing the United States' domestic sovereign immunity). In narrowing the waiver for non-commercial torts to require the presence in the United States of a human tortfeasor, the district court erred.

3. Exempting torts committed by remotely owned or operated instrumentalities would undermine the FSIA's remedial purpose.

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, including remote controlled devices. For example, unmanned aerial vehicles, *i.e.*, drones, were already in extensive use during the Vietnam

War, flying surveillance sorties in foreign sovereign territory.[38] And while the drafters of the FSIA might not have anticipated cyberattacks and spyware, 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.[39] 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.

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. In the coming years, foreign states will likely operate self-driving cars in U.S. territory. And it is already "possible to hack remotely into a car's electronics" and cause a

---

[38] *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.

[39] 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* http://www.start.umd.edu/sites/default/files/files/publications/br/Background_Report_2011JanuaryPackageIncendiariesMD.pdf

"crash from thousands of miles away." JA687.[40] Whether it is through spyware, unmanned drones, or self-driving cars, foreign states can and do cause injuries to Americans on American soil. Technology may have rendered the human agent unnecessary, but clearly the foreign state has still engaged in tortious activities in U.S. territory. And that was the problem Congress sought to remedy. For the FSIA tort exception to continue to serve its remedial purpose, courts must apply it to these factual scenarios.

E. Mr. Kidane's interpretation and application of the entire tort rule prevents absurd results.

It would be absurd to find that a cyber-trespass occurred overseas for purposes of the FSIA tort exception, but inside the United States for purposes of the substantive violation. But that is exactly what would happen if the decision below were affirmed.

As discussed *supra*, every court that has examined the issue has held that the place of interception determines whether the Wiretap Act is being applied domestically or extraterritorially. It would contradict this whole

---

[40] *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/.

line of authority to hold that the wiretapping of Mr. Kidane's Skype calls in Maryland did not "occur[] within the territorial jurisdiction of the United States," *Amerada Hess*, 488 U.S. at 441.

Affirming the district court would also conflict with an emerging rule, across a spectrum of computer intrusion cases, that remote intrusions occur at the location of the trespassed device or data. For example, the Second Circuit recently held that the Stored Communications Act ("SCA"), only applied to the accessing of data stored in the United States because it lacked clear extraterritorial effect. *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 212 (2d Cir., 2016). The Second Circuit found that the "'focus' of the SCA is privacy, and the relevant territorial locus of the privacy interest is where the customer's protected content is stored." *Id.* at 222 n.1 (Lynch, J., concurring). Similarly, a leading opinion on the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4), found that the statute was violated in U.S. territory when a Russian hacker remotely accessed computers within the United States: "The fact that . . . computers were accessed by means of a complex process initiated and controlled from a remote location does not alter the fact that the accessing of the computers . . . [that was] prohibited

by the statute, occurred at the place where the computers were physically located." *United States v. Ivanov*, 175 F. Supp. 2d 367, 371 (D. Conn. 2001).

Similarly, courts ruling on conflict of laws and personal jurisdiction issues have held that remote, computer-access torts occur at the site of the trespassed computer. *See, e.g.*, *MacDermid, Inc. v. Deiter,* 702 F.3d 725, 728 (2d Cir. 2012) (holding that a Canadian resident who "physically interacted only with computers in Canada" was subject to personal jurisdiction in Connecticut because she accessed computer servers located in that state to obtain confidential data); *Am. Online, Inc. v. Nat'l Health Care Disc., Inc.*, 121 F .Supp. 2d 1255, 1270 (N.D. Iowa 2000) (finding, for choice of law purposes, that Virginia was the *situs* of an Iowa corporation's unauthorized access of AOL computers located in Virginia).

In sum, Ethiopia waived its immunity under the FSIA tort exception when the FinSpy software module, under Ethiopia's exclusive use and control, intercepted Mr. Kidane's Skype calls, and monitored his emails, web browsing, and other private data located on his computer in Silver Spring, Maryland. Those precipitating acts occurred entirely in the United States. By stepping outside the four corners of the tort exception, and considering preparatory acts and requiring the physical presence of a

tortfeasor, the district court took it upon itself to narrow the non-commercial tort exception. This Court should reverse that error and avoid the absurd result that the remote wiretapping of a U.S.-based computer occurs in the United States if done by a private person, but overseas if done by a foreign state.

Issue Two – Wiretap Act

Standard of Review

A "pure legal question of statutory interpretation" is reviewed *de novo*. *Validus Reinsurance, Ltd. v. United States*, 786 F.3d 1039, 1042 (D.C. Cir. 2015)

II. The Wiretap Act creates a civil cause of action against governmental entities, including foreign sovereigns, for unlawful interceptions.

In passing the Wiretap Act, Congress created a statutory regime providing both civil and criminal sanctions for the surreptitious interception of Americans' communications. Certain courses of conduct give the federal government a civil cause of action, while other courses of conduct serve as the basis for a private right of action. *Compare* 18 U.S.C. § 2511(5) and § 2520(a). Similarly, some defendants ("any person") can be subject to criminal penalties while a larger set ("person or entity, other than

the United States") may face civil liability for the same conduct. *Compare* § 2511(1) and § 2520(a).

Ethiopia, as a foreign sovereign, is not a "person" subject to criminal liability under the Wiretap Act. However, as a governmental "entity" within the meaning of the Wiretap Act, Ethiopia ***is*** a proper civil defendant. And it can be sued under § 2520(a) for interceptions in violation of § 2511(1)(a) that its agents carried out while acting in their official capacity. The district court erred by finding otherwise. That error should be reversed because the text, structure, history, and purpose of the Wiretap Act all show that Congress intended to make governmental entities, other than the United States, civilly liable for their agents' unlawful interceptions.

A. The Wiretap Act provides a civil remedy for unlawful interceptions against all persons or entities, other than the United States.

The Wiretap Act provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a). The plaintiff may sue "the person or entity, other than the United States, which engaged in that violation." *Id.* The syntax and structure of Section 2520

unequivocally show that any "entity, other than the United States," can be sued for any of the three enumerated violations: the interception, disclosure, or intentional use of a "wire, oral, or electronic communication." The latter clause, "engaged in that violation," clearly refers to the preceding clause, "intercepted, disclosed, or intentionally used." And the remedy is framed in broad terms, without any words of limitation save the specific exemption of the United States. Thus the plain meaning of the text is that all persons or entities "other than the United States" are subject to suit for any of three courses of prohibited conduct, including interceptions.

1. The term "entity" includes governmental entities.

When first enacted in 1968, section 2520 authorized recovery only against the "person" who violated the Wiretap Act. Entities falling outside the section 2510 definition of "persons" were not subject to private civil suits for committing unauthorized interceptions of Americans' communications.[41] In 1986, however, Congress enacted the Electronic

[41] The Act defines a "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

Communications Privacy Act ("ECPA"), Pub. L. No. 99–508, § 103, 100 Stat. 1848, which amended section 2520 to "add[] the words 'or entity' to those who may be held liable under the Act." *Adams v. City of Battle Creek*, 250 F.3d at 980, 985 (6th Cir. 2001).

Although the term "entity" is undefined, every court to consider the issue—including the court below—has held that "a governmental entity may be liable in a civil suit under the Act." *Adams*, 250 F.3d at 985; *see also Seitz v. City of Elgin*, 719 F.3d 654, 657 (7th Cir. 2013) ("entity . . . includes government units"); *Organizacio JD Ltda. v. U.S. Dep't of Justice*, 18 F.3d 91, 94–95 (1994). These courts correctly reason that the plain meaning of "entity" includes governments. *Black's Law Dictionary* 477 (5th ed. 1979). And if "entity" were limited to business associations, then the 1986 amendments to § 2520 would have added nothing because the definition of "person" already included such organizations. *See Organizacion JD Ltda.*, 18 F.3d at 94–95.

That governmental entities can be sued under § 2520 is underscored by the fact that in 2001, Congress amended § 2520 in the PATRIOT Act "to exclude the United States from entities that could be liable." *Williams v. City of Tulsa*, 393 F. Supp. 2d 1124, 1132–33 (N.D. Okla. 2005). This "evidences a

Congressional understanding that the 1986 amendment created governmental liability." *Id.*; *see also Garza v. Bexar Metro. Water Dist.*, 639 F. Supp. 2d 770, 774 (W.D. Tex. 2009) ("There would have been no reason for Congress to carve out an exception for the United States if governmental entities could not be sued under the statute."). The government of Ethiopia is undoubtedly a governmental entity.

2. An "entity" includes a foreign state and its agencies and instrumentalities.

As a governmental entity, a foreign state may be sued under § 2520 provided it is not entitled to immunity under the FSIA. This is so for two reasons. First, Congress identified the unlawful surveillance activities of foreign states as an evil the ECPA sought to remedy in 1986, when it imposed civil liability on "entities." Although the Act does not explicitly reference foreign states, its legislative history shows that Congress was alarmed at foreign states' ability to intercept electronic communications in the United States. The House Report observed that the "interception of microwave transmissions" is "well known as to be an option for . . . foreign intelligence agencies." H.R. Rep. 99–647, at 19–20 (1986). It was wrong then for the district court to conclude that Congress did not "intend to subject

foreign states to suit in U.S. courts under the Wiretap Act." JA672. Congress was evidently concerned with interceptions by foreign intelligence agencies at the time the ECPA was enacted.

What's more, if Congress had intended to exclude foreign states from suit, it would have said so when it carved out an exception for the United States in the PATRIOT Act. The FSIA was a decade old when the ECPA extended civil liability for wiretapping to entities and Congress surely would have been aware of this possibility by 2001. The inclusion of a safe harbor for the United States is, by negative implication, the exclusion of any safe harbor for foreign states.

3. An entity can only "engage" in a violation through the acts of its agents, officials, or employees.

Courts must give meaning and effect to every word in a statute. *Corley v. United States*, 556 U.S. 303, 304 (2009) ("[A] statute should be construed [to give effect] to all its provisions, so that no part will be inoperative or superfluous, void or insignificant.") (citation omitted). Here section 2520 states that an aggrieved party may seek recovery from the "person or entity . . . , which engaged in [a] violation" of the Wiretap Act. An "entity"—whether governmental or otherwise—is a legal fiction. It cannot physically

perform any of the conduct regulated by the Wiretap Act. It cannot directly tap a phone line, disclose user communications, or use confidential information. As the district court recognized, such entities act through their agents, officials, or employees. *See* JA678.

To give meaning and effect to § 2520's reference to entities engaging in violations, the terms "engaged in" must be read to include an entity engaging vicariously in unlawful interceptions performed in an official capacity by its agents, officials, or employees. Any other reading makes the term "entity" superfluous, because an "entity" cannot directly perform the *actus reus* of any Wiretap Act violation. This is as true for legal persons such as corporations within the meaning of § 2510(6) as it is for an entity. As the district court observed: "Because these entities can act only through their . . . agents . . ., the definition necessarily already encompasses a concept of agent-principal or vicarious liability." JA678.

But the district court failed to extend that necessary concept of vicarious liability to governmental entities, relying instead on inapposite precedent. In *Cicippio-Puleo v. Islamic Republic of Iran*, 353 F.3d 1024, 1036 (D.C. Cir. 2004), this Court declined to imply a cause of action against a foreign state. But that case dealt with a statute—the Flatow Amendment to

the FSIA terrorism exception—whose cause of action was explicitly limited to claims against a foreign official, employee, or agent, not against the foreign state itself. Here, in contrast, section 2520 expressly creates a cause of action against entities. So *Cicippio-Puleo* says little about the issue at hand.

More on point is the Supreme Court's longstanding rule that a public officer's official acts are effectively acts of state, and a "judgment against a public servant 'in his official capacity' imposes liability on the entity that he represents provided, of course, the public entity received notice and an opportunity to respond." *Brandon v. Holt*, 469 U.S. 464, 471–72 (1985); *see also Kentucky v. Graham*, 473 U.S. 159, 166 (1985) ("[A]n official-capacity suit is, in all respects other than name, to be treated as a suit against the entity. It is not a suit against the official personally, for the real party in interest is the entity.") (citation omitted).

When Congress amended section 2520 to impose liability on "entities" in 1986, it surely would have been aware of the Supreme Court's pronouncements in 1985, which made clear that an officer's tortious liability could be imputed to the entity she represents. Thus, the text of the statute makes clear that the term "entity" includes governmental entities

and that entities can "engage" in a violation through the official acts of their officers, agents, or officials. As a governmental entity, Ethiopia can be sued under § 2520 for its agents' interceptions in violation of § 2511(1). The district court erred in holding otherwise.

B. The district court erred in finding that no Wiretap Act violation occurred.

After agreeing with Appellant that section 2520 creates a right of action against governmental entities, the lower court erred in its finding that Ethiopia did not actually violate the Wiretap Act. JA678.

In this case, an agent of the Federal Democratic Republic of Ethiopia was responsible for the installation of FinSpy on Mr. Kidane's computer in Maryland, which intercepted Mr. Kidane's communications. JA448-49. Under the district court's holding, Mr. Kidane could have pursued a Wiretap Act claim against that unknown agent of Ethiopia, but not against that agent's principal. That holding is contrary to the text and history of the statute as well as its goal—to give Americans like Mr. Kidane recourse when their communications are unlawfully intercepted.[42]

[42] Moreover, if Mr. Kidane had sued an agent of Ethiopia in his official capacity, we would reach the same circular result: under *Brandon*, 469 U.S. at 471–72, liability would still flow to Ethiopia for the official acts of its

The district court based its holding on a flawed reading of § 2520. Although the district court agreed that a governmental entity is an "entity" under § 2520, it reasoned that an entity is only amenable to suit for violations of § 2511(1) for which the entity itself could be criminally prosecuted. *See* JA675, JA678. Since § 2511(1) only imposes criminal sanctions for unlawful interceptions on a "person," the court concluded that an "entity" cannot violate § 2511(1) and hence cannot be held liable for an interception. JA678.

Under this narrow reading of the statute, an entity could only be held civilly liable for one single violation out of the entire range of the Wiretap Act's prohibited conduct: a violation of § 2511(3)(a). This section specifies that "entities" which provide electronic communication services to the public violate the Wiretap Act if they intentionally divulge the contents of those communications. By including "or entity" in section 2511(3)(a) but not in 2511(1), according to the district court, an "entity" can only be held liable for, presumably, disclosures, not interceptions. But this cuts against

---

agent. If the Court agrees that that circle must be closed, it should remand this case and instruct the district court to give plaintiffs leave to amend the Complaint to include individual Ethiopian officials as defendants.

the weight of authority and collapses the Wiretap Act's distinction between criminal and civil sanctions.

1. The weight of authority subjects governmental entities to liability for interceptions.

The district court's reading ignores the case law it otherwise cites with approval. For instance, in *Adams v. City of Battle Creek,* 250 F.3d 980 (6th Cir. 2001), the plaintiff named both a governmental entity and an employee of that entity as defendants in a Wiretap Act claim for the interception of his pager messages. The specific issue before the Sixth Circuit was whether the governmental entity defendant (and not just its human agent) could indeed be liable for an *interception* of the plaintiff's communications. *Id*. at 985. The court held that it could. *Id*. As another court observed, Congress "amended § 2520 to add that an aggrieved party could recover from an *intercepting* 'person or entity, other than the United States.'" *Williams v. City of Tulsa. OK*, 393 F. Supp. 2d 1124, 1132 (N.D. Okla. 2005) (emphasis added).

Indeed, courts around the country have regularly permitted Wiretap Act claims for interception under section 2511(1) to proceed against governmental entities. *See, e.g., Organizacion JD Ltda. V. U.S. Dep't of Justice*, 18 F.3d 91, 94–95 (2d Cir. 1994) (claim for Wiretap Act interception);

Williams, 393 F. Supp. 2d at 1132 (same); *Conner v. Tate*, 130 F. Supp. 2d 1370, 1373–75 (N.D. Ga. 2001) (same); *Dorris v. Absher*, 959 F. Supp. 813, 820 (M.D. Tenn. 1997) (same) *aff'd in part, rev'd in part*, 179 F.3d 420 (6th Cir. 1999); *Garza v. Bexar Metro. Water Dist.*, 639 F. Supp. 2d 770, 774–775 (W.D. Tex. 2009) (same).

The district court erred in holding that claims for interception under section 2511(1) could only proceed against "persons" and not governmental entities, and indeed cited no authority for that proposition.

2. The district court misconstrued Congress's decision to exempt governmental entities from criminal penalties as a decision to insulate such entities from civil liability.

Courts interpreting the Wiretap Act draw a distinction between *criminal* liability under Section 2511 of the Act, which applies only to "persons," and *civil* liability under Section 2520, which is more expansive and includes governmental entities. *Conner*, 130 F. Supp. 2d at 1373–75.

This distinction lies in the structure of the Wiretap Act. The Act first defines certain conduct as prohibited or permitted. § 2511(1). Then it prescribes which penalties attach, for what violations, and against whom. § 2511(4) (criminal penalties), § 2511(5) and § 2520 (civil liability). Section 2511 prohibits certain conduct including: interceptions, § 2511(1)(a);

disclosures of intercepted communications, § 2511(1)(c); and the unlawful divulging of the contents of a communication by an electronic communications service provider, § 2511(3)(a). Although all of these courses of conduct violate the Wiretap Act, not all of them carry the same penalties. Sections 2511(1),(4), and (5) impose criminal penalties only on a "person." In contrast, section 2520 imposes a more expansive civil liability on any "person or entity, other than the United States" for any "intercept[ion], disclos[ure], or intentional[] use" including a violation of section 2511(3)(a) (regulating electronic communications service providers), which carries no criminal penalties at all. Thus, Congress calibrated which penalties attach to which violations and against which actors.

The district court erred by collapsing these distinctions and implicitly holding that civil liability under § 2520 can only attach to violations of § 2511(3)(a) or in cases where the defendant would also be subject to criminal penalties under §2511(1). Congress intentionally uncoupled civil liability from criminal penalties. As the Senate Committee Report notes, "The plaintiff may bring a civil action under section 2520 whether or not the defendant has been subject to a criminal prosecution for the acts

complained of." S. Rep. 99-541, 27, 1986 U.S.C.C.A.N. 3555, 3581 (1986). That distinction should be left standing.

Finally, insulating governmental entities from both criminal and civil liability for unlawful interceptions cuts against one of Congress' main purposes in enacting and amending the Wiretap Act: regulating the surreptitious interception of Americans' communications. When Congress enacted the Wiretap Act and amended it in 1986, it sought "to guard against the arbitrary use of government power to maintain surveillance over citizens." H.R. Rep. 99-647, 16 (1986). Title I was specifically intended to "prohibit the interception of certain electronic communications." *Id.* Interception, and in particular interception by governmental actors, is at the heart of the Wiretap Act.

Accordingly, this Court should reverse the decision below and hold that the Wiretap Act provides a cause of action against governmental entities, including foreign states, that engage, by and through their officers, agents, and officials, in the interception of electronic communications in violation of the Wiretap Act.

CONCLUSION

For the reasons set forth herein, Mr. Kidane respectfully requests that this Court reverse the judgment of the district court, find that the district court has subject matter jurisdiction, and remand the case for further proceedings.

Respectfully submitted,

/s/ Richard M. Martinez
Richard M. Martinez
Samuel L. Walling
ROBINS KAPLAN LLP
800 LaSalle Avenue, Ste. 2800
Minneapolis, MN 55402
(612) 349-8500
(612) 339-4181
rmartinez@robinskaplan.com

Nathan Cardozo
Cindy Cohn
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436–9333

Scott A. Gilmore
Guernica 37 Int'l Justice Chambers
Premier House, 3rd Floor
12-13 Hatton Garden
London, U.K EC1N 8AN
+1 (510) 374-9872

Counsel for Plaintiff-Appellant John Doe

STATUTORY ADDENDUM

28 U.S.C. § 1603

For purposes of this chapter—

(a) A "foreign state", except as used in section 1608 of this title, includes a political subdivision of a foreign state or an agency or instrumentality of a foreign state as defined in subsection (b).

(b) An "agency or instrumentality of a foreign state" means any 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.

(c) The "United States" includes all territory and waters, continental or insular, subject to the jurisdiction of the United States.

(d) A "commercial activity" means either a regular course of commercial conduct or a particular commercial transaction or act. The commercial character of an activity shall be determined by reference to the nature of the course of conduct or particular transaction or act, rather than by reference to its purpose.

(e) A "commercial activity carried on in the United States by a foreign state" means commercial activity carried on by such state and having substantial contact with the United States.

28 U.S.C. § 1605

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

(1) in which the foreign state has waived its immunity either explicitly or by implication, notwithstanding any withdrawal of the waiver which the foreign state may purport to effect except in accordance with the terms of the waiver;

(2) in which the action is based upon a commercial activity carried on in the United States by the foreign state; or upon an act performed in the

United States in connection with a commercial activity of the foreign state elsewhere; or upon an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States;

(3) in which rights in property taken in violation of international law are in issue and that property or any property exchanged for such property is present in the United States in connection with a commercial activity carried on in the United States by the foreign state; or that property or any property exchanged for such property is owned or operated by an agency or instrumentality of the foreign state and that agency or instrumentality is engaged in a commercial activity in the United States;

(4) in which rights in property in the United States acquired by succession or gift or rights in immovable property situated in the United States are in issue;

(5) not otherwise encompassed in paragraph (2) above, 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; except this paragraph shall not apply to—

(A) any claim based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused, or

(B) any claim arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights; or

(6) in which the action is brought, either to enforce an agreement made by the foreign state with or for the benefit of a private party to submit to arbitration all or any differences which have arisen or which may arise between the parties with respect to a defined legal relationship, whether contractual or not, concerning a subject matter capable of settlement by arbitration under the laws of the United States, or to confirm an award made pursuant to such an agreement to arbitrate, if (A) the arbitration takes place or is intended to take place in the United States, (B) the agreement or award is or may be governed by a treaty or other international agreement in force for the United States calling for the recognition and enforcement of arbitral awards, (C) the underlying claim,

save for the agreement to arbitrate, could have been brought in a United States court under this section or section 1607, or (D) paragraph (1) of this subsection is otherwise applicable.

(b) A foreign state shall not be immune from the jurisdiction of the courts of the United States in any case in which a suit in admiralty is brought to enforce a maritime lien against a vessel or cargo of the foreign state, which maritime lien is based upon a commercial activity of the foreign state: Provided, That—

(1) notice of the suit is given by delivery of a copy of the summons and of the complaint to the person, or his agent, having possession of the vessel or cargo against which the maritime lien is asserted; and if the vessel or cargo is arrested pursuant to process obtained on behalf of the party bringing the suit, the service of process of arrest shall be deemed to constitute valid delivery of such notice, but the party bringing the suit shall be liable for any damages sustained by the foreign state as a result of the arrest if the party bringing the suit had actual or constructive knowledge that the vessel or cargo of a foreign state was involved; and

(2) notice to the foreign state of the commencement of suit as provided in section 1608 of this title is initiated within ten days either of the delivery of notice as provided in paragraph (1) of this subsection or, in the case of a party who was unaware that the vessel or cargo of a foreign state was involved, of the date such party determined the existence of the foreign state's interest.

(c) Whenever notice is delivered under subsection (b)(1), the suit to enforce a maritime lien shall thereafter proceed and shall be heard and determined according to the principles of law and rules of practice of suits in rem whenever it appears that, had the vessel been privately owned and possessed, a suit in rem might have been maintained. A decree against the foreign state may include costs of the suit and, if the decree is for a money judgment, interest as ordered by the court, except that the court may not award judgment against the foreign state in an amount greater than the value of the vessel or cargo upon which the maritime lien arose. Such value shall be determined as of the time notice is served under subsection (b)(1). Decrees shall be subject to appeal and revision as provided in other cases of admiralty and maritime jurisdiction. Nothing shall preclude the plaintiff in any proper case from seeking relief in personam in the same action brought to enforce a maritime lien as provided in this section.

(d) A foreign state shall not be immune from the jurisdiction of the courts of the United States in any action brought to foreclose a preferred mortgage, as defined in section 31301 of title 46. Such action shall be brought, heard, and determined in accordance with the provisions of chapter 313 of title 46 and in accordance with the principles of law and rules of practice of suits in rem, whenever it appears that had the vessel been privately owned and possessed a suit in rem might have been maintained.

[(e) , (f) Repealed. Pub. L. 110–181, div. A, title X, § 1083(b)(1)(B), Jan. 28, 2008, 122 Stat. 341.]

(g) Limitation on Discovery.—

(1)In general.—

(A) Subject to paragraph (2), if an action is filed that would otherwise be barred by section 1604, but for section 1605A, the court, upon request of the Attorney General, shall stay any request, demand, or order for discovery on the United States that the Attorney General certifies would significantly interfere with a criminal investigation or prosecution, or a national security operation, related to the incident that gave rise to the cause of action, until such time as the Attorney General advises the court that such request, demand, or order will no longer so interfere.

(B) A stay under this paragraph shall be in effect during the 12-month period beginning on the date on which the court issues the order to stay discovery. The court shall renew the order to stay discovery for additional 12-month periods upon motion by the United States if the Attorney General certifies that discovery would significantly interfere with a criminal investigation or prosecution, or a national security operation, related to the incident that gave rise to the cause of action.

(2)Sunset.—

(A) Subject to subparagraph (B), no stay shall be granted or continued in effect under paragraph (1) after the date that is 10 years after the date on which the incident that gave rise to the cause of action occurred.

(B) After the period referred to in subparagraph (A), the court, upon request of the Attorney General, may stay any request, demand, or order for discovery on the United States that the court finds a substantial likelihood would—

(i) create a serious threat of death or serious bodily injury to any person;

(ii) adversely affect the ability of the United States to work in cooperation with foreign and international law enforcement agencies in investigating violations of United States law; or

(iii) obstruct the criminal case related to the incident that gave rise to the cause of action or undermine the potential for a conviction in such case.

(3)Evaluation of evidence.—

The court's evaluation of any request for a stay under this subsection filed by the Attorney General shall be conducted ex parte and in camera.

(4)Bar on motions to dismiss.—

A stay of discovery under this subsection shall constitute a bar to the granting of a motion to dismiss under rules 12(b)(6) and 56 of the Federal Rules of Civil Procedure.

(5)Construction.—

Nothing in this subsection shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States.

18 U.S.C. § 2510

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of

obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)

(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a)

(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public

shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the

certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)

(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)

(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)

(a)(i) If the communication is—

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection—

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify the following:

This brief complies with the type-volume limitation of Rule 32(a)(7)(B) of the Federal Rules of Appellate Procedure and D.C. Circuit Rule 32(a)(3)(B) because this brief contains 12,193 words, excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii) of the Federal Rules of Appellate Procedure and Circuit Rule 32(a)(2). This brief complies with the typeface requirements of Rule 32(a)(5) of the Federal Rules of Appellate Procedure and the type style requirements of Rule 32(a)(6) of the Federal Rules of Appellate Procedure because this brief has been prepared in a proportionally spaced typeface using the 2010 version of Microsoft Word in 14 point Book Antiqua.

/s/ Richard M. Martinez
Richard M. Martinez

United States Court of Appeals
for the District of Columbia Circuit
John Doe, a.k.a. Kidane v. Federal Democratic Republic of Ethiopia
2016-7081

CERTIFICATE OF SERVICE

I, Richard M. Martinez, being duly sworn according to law and being over the age of 18, upon my oath depose and say that:

I am counsel for Appellant and am authorized to electronically file the foregoing FINAL OPENING BRIEF FOR APPELLANT with the Clerk of Court using the CM/ECF System, which will serve via e-mail notice of such filing to all counsel registered as CM/ECF users, including any of the following:

Robert P. Charrow
Laura Metcoff Klaus
Thomas R. Snider
Greenberg Traurig LLP
2101 L St NW #1000,
Washington, DC 20037
Counsel for Appellees

December 27, 2016

/s/ Richard M. Martinez
Richard M. Martinez