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,

Defendant-Appellee.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA CASE NO. 1:14-CV-00372,
JUDGE RANDOLPH D. MOSS

FINAL REPLY BRIEF OF APPELLANT

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

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

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

Statutes

Other Authorities

GLOSSARY OF ABBREVIATIONS

JASTA	Justice Against Sponsors of Terrorism Act
FSIA	Foreign Sovereign Immunities Act
FTCA	Federal Tort Claims Act
MLAT	Mutual Legal Assistance Treaty

SUMMARY OF THE ARGUMENT

First, the Complaint provides that the tortious acts that affected Mr. Kidane – the interception of his communications and the intrusions into his private Internet activities as well as those of his family – happened in his home in Maryland. FSIA case law, as well as the Wiretap Act case law, provide that the location of the act of interception and intrusion determines whether liability attaches. Here, that location is in Maryland.

Second, this Court should reject Ethiopia's invitation for it reach the discretionary-function argument that was not reached by the District Court, and to do so by relying on factual assertions about its motivations for wiretapping Mr. Kidane that were not raised in the briefing below. If it decides to reach this argument, the Court should find that Ethiopia does not have the discretion to ignore the mandatory channels of cooperation between nations with regard to highly regulated activities such as government wiretapping. Moreover, this Court should reject Ethiopia's attempt to have it create a foreign state national security exception to the FSIA.

Third, Ethiopia has not demonstrated that international law requires the Court to require physical human presence in the United States in order to apply the noncommercial tort exception to the FSIA, or that, even if it does, Congress has adopted this rule when in fact, it specifically failed to adopt it in the FSIA.

Fourth, as the District Court did, this Court should dismiss Ethiopia's claim that the tort claims here are based on deceit or misrepresentations, since neither cause of action requires those elements.

Finally, this Court should side with the great weight of authority that provides, first that governmental entities do have liability under the Wiretap Act and second, that the Wiretap Act does not preempt more restrictive state laws, such as Maryland's intrusion upon seclusion tort.

ARGUMENT

I. THE TORTS PLEADED WERE LOCATED ENTIRELY WITHIN THE UNITED STATES

Courts around the country, including this Court, have drawn a clean line in interpreting the FSIA between noncommercial tortious *acts* within the United States and those acts occuring outside the United States but whose *effects* are felt here. In *Letelier v. Republic of Chile*, 488 F.Supp. 665 (D.D.C. 1980), liability attached for an act of assassination in Washington DC, despite the fact that it was planned and commanded from abroad. In contrast, in *Jerez v. Republic Cuba*, 775 F.3d 419 (D.C. Cir. 2015), Cuba was held to be immune from suit for the act of torturing a Cuban refugee in Havana, despite the fact that the plaintiff suffered ongoing *effects* of the tort in the United States. When the tortious act occurs in the U.S., liability attaches. When the tortious act occurs outside the U.S., liabilty does not attach, even if some of the effects do occur here.

This case is clearly on the "act occurs in the U.S." side of the line. The acts here were the tortious capture of Mr. Kidane's voice calls and Internet activites, all of which occurred in his home in Maryland . *See* Appellant's Opening Brief ("Br.") at 8-23, Deferred Joint Appendix ("JA") at JA448.

A. THE ENTIRE TORT RULE EXAMINES ONLY WHERE THE TORTIOUS "ACT" OCCURRED, NOT WHERE IT WAS PLANNED, COMMANDED, OR DIRECTED

Ethiopia's brief disregards the central facts; at all relevant times, Mr. Kidane was located in the United States, the instrumentality of the torts—the FinSpy software—was located in the United States, and the tortious activity that gave rise to this suit—the interception of his communications—was accomplished entirely within the United States and indeed within Mr. Kidane's home in Silver Spring, Maryland. Those facts distinguish this case from each of the cases cited by Ethiopia.[1] For instance, the Supreme Court in *Amerada Hess* addressed an incident

[1] *Argentine Rep. v. Amerada Hess*, 488 U.S. 428 (1989) (plaintiff's vessel attacked while located in international waters off the Falkland Islands); *Persinger v. Islamic Republic of Iran*, 729 F. 2d 835 (D.C. Cir. 1984) (plaintiff taken hostage while located in Tehran); *Jerez v. Republic Cuba*, 775 F.3d 419 (D.C. Cir. 2015) (plaintiff tortured and injected with the hepatitis C virus while located in Cuba); *Cicippio v. Islamic Republic of Iran*, 30 F.3d 164 (D.C. Cir. 1994) (plaintiff taken hostage while located in Tehran); *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517 (D.C. Cir. 1984); *In re Terrorist Attacks on Sept. 11, 2001*, 714 F.3d 109, 117 (2d Cir. 2013) (While this case stems from the September 11 attacks, the actual torts alleged were the funding of Al Qaeda which occurred within Saudi Arabia. Plaintiffs did not "allege that any employees of [defendants]—or anyone controlled by these entities—committed a tortious act in the United States."); *O'Bryan v. Holy See*, 556 F.3d 361, 386 (6th Cir. 2009) (claim for negligent supervision of Catholic priests barred to the extent that the supervision occurred abroad, but allowed to the extent that it occurred within the United States); *Cabiri v. Gov't of Republic of Ghana*, 165 F.3d 193, 199 (2d Cir. 1999) (holding that this particular claim for intentional infliction of emotional distress was in essence a claim for misrepresentation and therefore barred by 28 U.S.C. § 1605(a)(5)(B), mentioning only in passing that the FSIA permits only claims for torts occurring within the United States); *Jones v. Petty-Ray Geophysical Geosource, Inc.*, 954 F.2d 1061, 1065 (5th Cir. 1992) (plaintiff killed

that occurred in the South Atlantic and this Court in *Persinger* examined the Iranian hostage crisis. *See e.g. Argentine Rep. v. Amerada Hess*, 488 U.S. 428 (1989); *Persinger v. Islamic Republic of Iran*, 729 F. 2d 835 (D.C. Cir. 1984). Unsurprisingly, both courts held that FSIA's noncommercial tort exception did not apply, since neither event occurred on U.S. soil. In none of the cases Ethiopia cites was the plaintiff in America when tortious activity took place.

Indeed, this case is no more a trans-boundary tort case than the seminal case of FSIA jurisprudence, *Letelier v. Republic of Chile*, 488 F.Supp. 665 (D.D.C. 1980). In *Letelier* the survivors of an assassinated Chilean dissident and his assistant brought a wrongful death suit against a number of individual defendants as well as the Republic of Chile. *Id*. at 665-66, n. 1. The Republic of Chile was accused of planning, commanding, and directing Mr. Letelier's assassination via car bomb at the hands of the individual defendants who were mostly Cuban agents, with at least one American assisting. *Id*.

The *Letelier* court accepted the plaintiffs' apparently undisputed (and indisputable) assertion that the tort—wrongful death—occurred where the car bomb went off in the District of Colombia. *Id*. It was of no moment that the

---

while located in Sudan); *Frolova v. Union of Soviet Socialist Republics*, 761 F.2d 370, 379 (7th Cir. 1985) (plaintiff's claim was based on her husband's detention while located in the USSR); *Olsen v. Gov't of Mexico*, 729 F.2d 641, 646 (9th Cir. 1984) (permitting a claim for negligence by pilot which included tortious acts located in both Mexico and the United States, contrasting a hypothetical that would be barred where *none* of the tortious conduct occurred in the United States).

defendant sovereign directed the tortious act from Santiago, Chile, sending commands to non-Chilean agents in the United States. The *acts* that Chile accomplished were the wrongful deaths of Mr. Letelier and his companion, not the issuance of the commands to initiate the assassination, and those torts were accomplished within the United States.

Ethiopia's suggestion that *Letelier* is no longer good law (Apellee Br. at 21) is entirely spurious and deeply troubling. First, this Court cited *Letelier* with approval in *MacArthur Area Citizens Association v. Republic of Peru*, 809 F.2d 918, 923 n.4 (D.C. Cir.), modified, 823 F.2d 606 (D.C. Cir. 1987). Second, if Ethiopia's framing of the entire tort rule were to become law, a foreign sovereign would be free to command or direct essentially any intentional tort within the United States, so long as the commands were issued abroad. Indeed, by painting *Letelier* as bad law, Ethiopia's argument implies that not only is it free to wiretap Americans without repercussion, but that it, or any other country, could hire assassins and send them into the United States to do their work without repercussion, so long as they were commanded from abroad. This Court should not accept Ethiopia's invitation.

Additionally, as noted above, Ethiopia's reliance on *Persinger* is misplaced. *Persinger v. Islamic Republic of Iran*, 729 F.2d 835, 842-43 (D.C. Cir. 1984). The focus of this Court's inquiry in *Persinger* was the Iran hostage crisis of 1979-81,

an event which took place in Tehran. The issue in *Persinger* was whether a United States embassy counted as the territory of the United States for the purposes of the FSIA: it does not. This Court therefore held that the noncommercial tort exception did not apply, as the *tortious acts* occurred in Tehran.

Ethiopia's cited portion of the *Persinger* decision, which distinguishes the "effects" of an act from the act itself, is beside the point. Appellee Br. at 13. Mr. Kidane does not allege merely that the "effects" of the wiretapping and tortious intrusion occurred in his home, he alleges that the intrusion and wiretapping acts themselves occurred in his home. Put another way, the torts alleged were not the issuance of the commands to wiretap Mr. Kidane, since those alone did nothing. The wiretap and intrusion occurred when Mr. Kidane's conversations and Internet activeies were intercepted by malware running on Mr. Kidane's computer. That occurred in his home *in Maryland*.

Finally, Appellee looks to the recently-enacted Justice Against Sponsors of Terrorism Act (the "JASTA") for support for its proposition that a foreign sovereign's agent abroad, directing a tort within the United States, is not within the noncommercial tort exception. 28 U.S.C. § 1605B(b). It provides none. Ethiopia is of course correct that the JASTA was an expansion of FSIA, but not by bringing externally commanded torts (involving terrorism, which of course is not the case here) into the FSIA. Rather, the JASTA chiefly expands FSIA with the addition of

a cause of action against those who provide "*indirect*" material support to those who commit terrorism within the United States. *Id*. (emphasis added). Previously, a cause of action was permitted only against those sovereigns which acted *directly* within the United States. If this suit were a complaint that Ethiopia indirectly financed the purchase of weapons (or for that matter malware) that were used by others to attack Mr. Kidane, then Ethiopia's argument might have weight. It does not. Here, Ethiopia acted directly within the United States through the acts of its specially designed, government-only spyware on Mr. Kidane's computer in Maryland.

B. THE "ACT" THAT FORMS THE BASIS OF THIS LAWSUIT WAS THE INTERCEPTION OF MR. KIDANE'S COMMUNICATIONS AND INTRUSION INTO HIS PRIVATE COMPUTER, NOT THE ISSUANCE OF THE COMMANDS THAT INITIATED THE SPYWARE

Ethiopia fundamentally misreads the Restatement (Second) of Torts § 2 (1977). As used in the Restatement, that the word "act" is used "to denote an *external manifestation* of the actor's will and does not include any of its results, even the most direct, immediate, and intended." *Id*. (emphasis added). As described in Appellant's opening brief and First Amended Complaint, the tortious act was the interception of Kidane's calls and the intrusion upon his seclusion caused by capturing his Internet activities. Phrased differently, the tortious operation of FinSpy on Kidane's computer was the *external manifestation* of

Appellee's will to track Mr. Kidane's communications. The results of that manifestation of Ethiopia's will was that Mr. Kidane's privacy in those communications was violated.

The initiating key strokes entered by the Ethiopian government agent that resulted in the activation of the FinSpy infection on Mr. Kidane's computer are akin to the commands sent to the Cuban agents by the government of Chile in *Letelier*. In both *Letelier* and the instant case, the commands sent by government agents abroad initiated the tortious acts within the United States, but those commands were not themselves the tortious acts.

Ethiopia confuses acts with effects. Hoping to construe the interception of Mr. Kidane's communications as the "effects" of the wiretap, Ethiopia glosses over the fact that interception is itself the act of wiretapping. And by mistaking acts for effects, Ethiopia contradicts the long settled rule under the Wiretap Act that the tortious "act" of wiretapping occurred where Mr. Kidane's computer was located in the U.S. and not in Ethiopia.

The *situs* of a Wiretap Act violation is the place where the interception occurs. *United States v. Cotroni*, 527 F.2d 708, 711 (2d Cir. 1975) ("[I]t is not the route followed by . . . communications which determines the application of [the Wiretap Act]; *it is where the interception took place*.") (emphasis added). And "an interception plainly occurs at or near the situs of the telephone" or computer where

"the contents" of the "communication are captured or redirected." *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992). As the Eleventh Circuit noted, "the term 'intercept' as it relates to 'aural acquisitions' refers to the place where a communication is initially obtained regardless of where the communication is ultimately heard." *United States v. Nelson*, 837 F.2d 1519, 1527 (11th Cir. 1988). Thus the interception that violated the Wiretap Act was committed entirely in the United States, by Ethiopia's recording device: "For § 2510(4) purposes, the recorder can be the agent of the ear." *United States v. Turk*, 526 F.2d 654, 658 n.2 (5th Cir. 1976).

Ethiopia errs by characterizing the actual interception of Mr. Kidane's communications as merely the "result" or "effect" of Ethiopia's tortious acts. Appellee Br. at 15-16. To the contrary, the interception *was* the tort. The result and effect of the tortious interception of Mr. Kidane's communications was the emotional distress and loss of privacy he suffered.

It is immaterial that Ethiopia engaged in collateral acts outside of the United States for two reasons. First, the Wiretap Act violation was complete when the FinSpy device intercepted Plaintiff's communications in Maryland. *See In re State Police Litig.*, 888 F. Supp. 1235, 1267 (D. Conn. 1995). Because interception occurs even prior to any human listening, it does not affect liability or jurisdiction that Ethiopia later transmitted, stored, or listened to recordings of Plaintiff's

communications outside of the United States. *See Rodriguez*, 968 F.2d at 136; *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) (Defendant's "failure to listen to the tapes should not insulate it from liability for the invasion of privacy it helped to occasion."); *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994). Thus, the torts at issue were complete upon interception and intrusion, both of which occurred entirely in the United States.

Second, federal courts have long recognized that a foreign state cannot defeat the FSIA's tort exception simply by alleging that it engaged in *some* foreign conduct, when the gravamen of the tort occurred on U.S. soil. For example, the Ninth Circuit held that the FSIA tort exception applied to wrongful death claims based on a Mexican prisoner-transport flight that crashed in the United States due to negligent piloting in the U.S. and negligent training in Mexico. *Olsen v. Gov't of Mexico*, 729 F.2d 641, 646 (9th Cir. 1984). Because at least one tort in the cross-border chain of events occurred in the United States, the tort exception was triggered. *Id*.

In rejecting the sort of logic-defying, artful pleading that Ethiopia displays here, the *Olsen* court observed: "requiring every aspect of the tortious conduct to occur in the United States . . . would encourage foreign states to allege that some tortious conduct occurred outside the United States." *Id*. This would "diminish the rights of injured persons seeking recovery" and undermine "the purpose of the

FSIA, which is to 'serve the interests of justice and . . . protect the rights of both foreign states and litigants in United States courts.'" *Id.* (quoting 28 U.S.C. § 1602).

Finally, the fact that the target of Ethiopia's malware appears not to have been Mr. Kidane originally is irrelevant; the tort alleged here is not the sending of the email, but rather the activation and maintenance of the spyware. In any case, the Complaint, which must be construed as true, alleges that once Mr. Kidane's computer was infected with FinFisher, Ethiopia intentionally maintained the infection with full knowledge of both Mr. Kidane's identity and location. JA440-41, JA447-48. This is confirmed by the fact that, after being caught red-handed by Citizen Lab and publicly exposed, Ethiopia then affirmatively acted to shut down the infection. *Id*.

The issue of whether torts occuring in the United States but initiated by digital agents rather than human ones are subject to liability under the FSIA is one of first impression—although this Court announced in dicta in *Jerez* that they are. 775 F.3d at 424. It would not expand FSIA for this Court to adopt its dicta from *Jerez* and hold that the entire tort rule may be satisfied without sending a human agent into the United States. To the contrary, it would represent a significant narrowing of the FSIA to adopt Ethiopia's proposed rule.

II. THE APPELLEE'S TORTIOUS CONDUCT AGAINST MR. KIDANE WAS NOT A DISCRETIONARY ACT

The District Court did not determine whether the discretionary-function exception bars Mr. Kidane's claims, and this Court should also decline to reach Ethiopia's argument on this point.

Ethiopia concedes that "the District Court did not render a decision on the applicability of the discretionary-function exception." Appellee Br. at 29. Accordingly, there is no decision for this Court to review and Appellee's argument should be disregarded. *Bowie v. Maddox*, 642 F.3d 1122, 1131 (D.C. Cir. 2011) ("a federal appellate court does not consider an issue not passed upon below"), quoting *Singleton v. Wulff*, 428 U.S. 106, 120 (1976).

The District Court declined to render a decision on the discretionary-function exception because it was "without the necessary record upon which to draw a conclusion regarding Ethiopia's conduct (and, accordingly, the applicability of the discretionary function exception)." JA701. Ethiopia all but concedes this point in citing to out-of-context evidence in support of its assertion that Ginbot-7 is deemed a terrorist organization by the Ethiopian government (while at the same time declining to stipulate to any facts injurious to its cause). Br. at 27. Ethiopia

neglects to note that this designation was "controversial", and has been criticized by both The Committee to Protect Journalists and Human Rights Watch.[2] JA468.

This appeal is not the time for Ethiopia to mine the record for helpful (out-of-context) facts that it failed to present below. Nor is this appeal the place to consider for the first time Ethiopia's contention that it was acting in its national security interests. Rather, this appeal is limited to the record developed and the arguments raised in the District Court. *Murphy Oil and Prod. Co. v. Dept. of the Interior*, 270 F.3d 957 at 958 (D.C. Cir. 2001) (citing *Ohio v. Environ. Protection Agency*, 997 F.2d 1520 at 1528-29 (D.C. Cir. 1983) for the "incontrovertible proposition that one may not present an argument on appeal without having first raised it below.").

Here, the District Court correctly observed that "in creating a discretionary function exception under the FSIA, Congress did not mean to shield 'discretionary' acts by foreign states when those acts involve serious violations of U.S. criminal

[2] Ethiopia also insists on citing to a 2010 U.S. State Department Human Rights Report for the assertion that "Member of Ginbot 7 have 'publicly advocated violent overthrow of the [Ehiopian] government.'". Appellee Br. at 27. Ethiopia neglects to note that this statement was made in the context of detailing reports that Ethiopia had physically abused and tortured members of Ginbot 7 in interrogations. *Id.* Ethiopia further fails to direct this Court to more-recent reports from the U.S. State Department, in which no mention of Ginbot 7 advocating violent overthrow is to be found. *See* U.S. State Department, 2014 Ethiopia Human Rights Report < http://www.state.gov/documents/organization/236570.pdf> (last visited December 7, 2016); U.S. State Department, 2015 Ethiopia Human Rights Report http://www.state.gov/documents/organization/252893.pdf (last visited December 7, 2016).

law." JA682. The court correctly followed this Circuit's guidance in *MacArthur*, 809 F.2d at 922 n.4, that the discretionary function exception does not shield serious criminal acts committed by foreign government agents. *Id. Accord Restatement (Third) of the Foreign Relations Law of the United States* § 454 n.3. And, while observing that the computer intrusion alleged here could constitute multiple serious criminal acts, the court correctly noted that the record below was insufficient to determine the precise criminal nature of Ethiopia's activities, and hence whether the discretionary-function exception applies. That remains true today. For this reason alone, the Court should decline to address Ethiopia's discretionary-function argument.

A. IF CONDUCTING WIRETAPPING IN THE TERRITORY OF ANOTHER STATE WERE A DISCRETIONARY ACT, IT WOULD RENDER SUPERFLUOUS THE MLAT SYSTEM

Should the Court elect to consider Appellee's discretionary-function argument, it should fail. Ethiopia has made no showing that it even attempted, much less succeeded in securing the U.S. government's authorization to wiretap Americans inside the U.S. — or more likely have the U.S. law enforcement wiretap for it. This court should not grant Ethiopia the discretion to ignore mandatory channels of cooperation between countries. *See Restatement (Third) of Foreign Relations Law* § 432(2) (1987) ("A state's law enforcement officers may

exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.").

Electronic surveillance of Americans by law enforcement and intelligence agencies in the United States is a highly regulated activity. Electronic surveillance by anyone else is a serious felony. From the Fourth Amendment's warrant requirements to the detailed procedures in 18 U.S.C. §§ 2510 et seq, to the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 *et seq.*, this country's elaborate frameworks for regulating surveillance aim to balance the needs of law enforcement (and occasionally intelligence agencies) with the constitutional rights, due process protections, privacy and civil liberties of Americans. Those legal rules are buttressed by complex internal procedures within the specific government agencies. This regulatory apparatus is not elective. To the contrary, it is the "exclusive means" for conducting electronic surveillance. 18 U.S.C. § 2511(2)(f); see also *In re NSA Telecomm. Records Litig.*, 564 F. Supp. 2d 1109, 1116 (N.D. Cal. 2008).

For Ethiopia or any foreign government to surveil U.S. citizens on U.S. soil, it must follow mandatory channels of cooperation. See *In re Premises Located at 840 140th Ave. NE, Bellevue, Wash.*, 634 F.3d 557, 562-64 (9th Cir. 2011) (discussing framework for letters rogatory and mutual legal assistance treaties ("MLATs")). None of those channels allows for unilateral wiretapping of

Americans in America; all require the consent and cooperation of the U.S. government. While Appellee and the United States have yet not entered into a mutual legal assistance treaty, this fact gives Appellee less—and certainly not more—discretion to conduct wiretapping of Americans in the United States.[3]

Moreover, any foreign law enforcement cooperation in U.S. territory would be subject to American guarantees of individual rights. *See id.* at 572 ("We therefore hold that, in the context of an MLAT request, a district court may not enforce a subpoena that would offend a constitutional guarantee."). Indeed, when Congress amended the Wiretap Act in the Electronic Communications Privacy Act of 1986, it sought to protect those guarantees by striking "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." S. Rep. No. 99–541, at 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555.

That balance would be undermined if foreign states such as Appellee were permitted to ignore the Wiretap Act's warrant requirements and eavesdrop on U.S. citizens in their homes at will, without fear of judicial scrutiny or liability. To give Appellee such discretion would perversely incentivize foreign states to *not* cooperate with U.S. law enforcement agencies — and thereby circumvent

[3] See U.S. Dept. of State Foreign Affairs Manual, 7 FAM 960 Criminal Matters (2013), available at <http://www.state.gov/documents/organization/86744.pdf>.

American privacy regulations and rule of law. Yet that is what Ethiopia maintains here.

Because Appellee and its agents had no discretion to conduct unauthorized law enforcement operations in U.S. territory, it does not enjoy immunity for illegal wiretapping and the invasion of Appellant's privacy.

B. THERE IS NO NATIONAL SECURITY EXCEPTION TO THE FSIA AND THIS COURT SHOULD NOT CREATE SUCH AN EXCEPTION, AS IT WOULD SWALLOW THE RULE

Appellee's newly conceived "national security" argument is also not supported by the record or the law and must be rejected.

First, there is no evidence whatsoever on the record regarding the Ethiopian government's motivation for wiretapping Appellant in his home and continuously monitoring his computer usage for four and a half months. Appellee belatedly alleges in its opposition that Appellant was assisting a political opposition group that it has branded a "terrorist organization" (it is not and the United States has not designated it as such).[4] Appelleee Br. at 27. But irrespective of the falseness of this claim, this is a factual issue that the Appellee failed to raise, much less prove, below. As a result, the record does not address and the District Court did not resolve this question, nor should it have done so on a motion to dismiss. Furthermore, there is also no evidence that this alleged fact, if true, is what

[4] *See* U.S. Dep't of State, *Foreign Terrorist Organizations*, http://www.state.gov/j/ct/rls/other/des/123085.htm

motivated Ethiopia to activate and maintain the FinSpy software and to thereby intercept Appellant's communications. If anything, this belatedly alleged fact more closely resembles a *post hoc* justification than a preconceived motivation.

Second, even if there were evidence of Appellee's motivation, there is no "national security" exception to the FSIA, nor should this Court create one here. Indeed this Court in an FTCA case, *Black v. Sheraton Corp. of Am.*, 564 F.2d 531, 541 (D.C. Cir. 1977) strongly suggested that there is no national security exception to the FTCA, on which the FSIA's discretionary function provision is modeled. *Letelier*, 488 F. Supp. at 673 ("As its language and the legislative history make apparent, the discretionary act exemption of subsection (A) corresponds to the discretionary act exception found in the Federal Tort Claims Act.").

Third, no FSIA case has inquired into the motivation of a tortious course of conduct—only into the nature of the act. The conduct in *Letelier* was clearly motivated by "national security," and, similar to here, a desire to quash a dissident in exile. Similarly, the conduct in *Liu* also contained elements that could be chracterized as a "national security" interest. But the defendants' motivations were of no bearing in either *Letelier* or *Liu*—both of which expressly declined to apply the discretionary-function exception. In *Letelier*, the court noted that even acts that may appear to be discreationary are not exempt as discretionary acts if they are illegal:

> While it seems apparent that a decision calculated to result in injury or death to a particular individual or individuals, made for whatever reason, would be one most assuredly involving policy judgment and decision and thus exempt as a discretionary act under section 1605(a)(5)(A), that exception is not applicable to bar this suit. As it has been recognized, there is no discretion to commit, or to have one's officers or agents commit, an illegal act.

488 F. Supp. at 673. *See also Liu v. Republic of China*, 892 F.2d at 1419, 1431 (9th Cir. 1989); Appellee Br. at 29 (noting courts' refusal in *Liu* and *Letelier* to apply the discrectionary-function exception to illegal acts.).

Finally, spying in the territory of another state is illegal. It is not "perfectly proper" to spy on citizens in another country as Appellee boldly suggests. When spies get caught, they go to jail regardless of whether their own country's law "permitted" their activities. For example, Aldrich Ames spied for Russia and, upon being caught and convicted, was sentenced to life in prison without the possibility of parole. *See* FBI "Aldrich Ames," https://www.fbi.gov/history/famous-cases/aldrich-ames. Consequently, the fact that Congress has authorized American intelligence agencies to conduct surveillance operations on foreign states, something that still requires compliance with complex procedures and policies, does not mean that Congress has authorized foreign states to conduct unfettered and unregulated surveillance operations in the United States. Unsurprisingly, Appellee cites no authority to support this troubling assertion.

Indeed, Appellee's discretionary-function argument advocates for a surveillance paradigm that is absurd on its face. Appellee acknowledges that American intelligence agencies are *prohibited* from spying on American citizens, but argues that foreign intelligence agencies who spy on American citizens are protected by the FSIA's discretionary-function exception. Appellee Br. at 30. Thus, adopting Appellee's interpretation of the discretionary-function exception would create a construct where *foreign* states can spy on American citizens with impunity, but the United States cannot. Surely that is not the balance Congress sought to strike in enacting the FSIA. Appellee's argument should be rejected

III. CONGRESS REJECTED THE PHYSICAL PRESENCE REQUIREMENT IN THE EUROPEAN CONVENTION ON STATE IMMUNITY

Ethiopia is simply wrong that international law requires this Court to graft a physical presence requirement onto the noncommercial tort exception.

First and foremost, Congress studied the European Convention on State Immunity ("European Convention") when it enacted the FSIA in 1976. Congress knew that this treaty's tort exception requires that "the author of the act or omission [be] present in that territory at the time of the act or omission." European Convention, Art. 11, reprinted in 1976 Hearings at 39. Yet Congress did not include a presence requirement in the noncommercial tort exception. If Congress had intended the FSIA to track the European Convention it would have done so.

Nevertheless, Ethiopia urges this Court to effectively rewrite the FSIA to conform to the European Convention and to the United Nations Convention on the Jurisdictional Immunities of States and their Property ("U.N. Convention"), G.A. Res. 59/38, Annex, U.N. Doc. A/RES/59/38, Art. 12 (Dec. 2, 2004). But that is a task for Congress, not this Court. And it would be a strange task, since the United States is not a party to either convention and neither gives proof of international custom. In 12 years, the U.N. Convention has not even garnered enough signatories to enter into force.[5] And the European Convention is a regional treaty, limited to Europe. These hardly reflect generally accepted customary norms.

Finally, Ethiopia has failed to cite a single foreign sovereign-immunity law from any foreign country that requires the physical presence of a flesh-and-blood tortfeasor in the jurisdiction of suit. True, several countries require that the tortious act occur within the forum state's territory. *See, e.g.*, UK State Immunity Act 1978, § 5 ("A State is not immune as respects proceedings in respect of – (a) death or personal injury; or (b) damage to or loss of tangible property, caused by an act or omission in the United Kingdom."). But a territorial act requirement is no bar to a tort accomplished within a state's territory by sending commands from abroad. If a state-sponsor of terrorism, such as Iran, were remotely to detonate a bomb in

[5] *See* United Nations Convention on the Jurisdictional Immunities of States and their Property, https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20III/III-13.en.pdf.

London, there is no reason to doubt a resulting death would be "caused by an act . . . in the United Kingdom." *Id.*

In short, the noncommercial tort exception reflects the judgment of Congress that the FSIA should *differ* in certain respects from international instruments such as the European Convention. The Court should not adopt a physical presence requirement that Congress declined to enact.

IV. THE TORT CLAIMS HERE ARE BASED ON DEFENDANT'S AFFIRMATIVE MISCONDUCT, NOT MISREPRESENTATION OR DECEIT

The District Court correctly found that Appellant's claims were not based on misrepresentation or deceit. JA682-83. Neither misrepresentation nor deceit are elements of the privacy torts at issue in this case and Ethiopia's claim that the fact that it "tricked" Mr. Kidane into opening an email attachment (perhaps rather than simply asking him to) is of no consequence.

Aside from cherry picking two words from the First Amended Complaint and misrepresenting them out of context, Appellee's factual and legal support for its argument is strikingly absent. The "trickery" alleged here is immaterial to the causes of action alleged.

Mr. Kidane's tort claims are not based on "misrepresentation" or "deceit." For example, to prove Mr. Kidane's claim for invasion upon seclusion, Mr. Kidane must prove (1) an intentional intrusion, physical or otherwise (2) upon the solitude

or seclusion of another or his private affairs or concerns (3) that would be highly offensive to a reasonable person. *See Schuchart v. La Taberna del Alabardero, Inc.*, 365 F.3d 33, 35–36 (D.C. Cir. 2004) (citing the Restatement (Second) of Torts § 652B). None of these elements requires misrepresentation or deceit. Rather, as noted above, Mr. Kidane's claims arise out of the Ethiopian government's affirmative acts of installing computer spyware software on Mr. Kidane's computer in the United States, and then having that spyware resident and operating on a U.S. computer intercept, record, and transmit from Maryland—back to Ethiopia—Mr. Kidane's private communications.

Courts interpreting section 1605(a)(5)(B), including the District Court below, often look to cases interpreting the Federal Tort Claims Act, since the exceptions in section 1605(a)(5)(B) mirror those in 28 U.S.C. § 2680(h). *See, e.g.*, *O'Bryan v. Holy See*, 556 F.3d 361, 385 (6th Cir. 2009) ("Courts generally have looked to the definition of misrepresentation in the FTCA as a guide for defining the term under the FSIA"). In addressing a very similar FTCA case, this Court rejected a claim for sovereign immunity, holding that under the FTCA, a claim for invasion of privacy by intrusion—based on "illegal eavesdropping"—is *not* barred under section 2680(h) as a "misrepresentation" based tort. *See Black v. Sheraton Corp. of Am.*, 564 F.2d 531, 541 (D.C. Cir. 1977). As the Court reasoned, "[s]ince the Tort Claims Act does not give immunity for the type of activity in which the

government was here alleged to be involved, *i.e.*, trespass and invasion of privacy, we hold that plaintiff's claim for damages arising therefrom is not barred." *Id.*

The District Court properly relied on *Black v. Sheraton* to find that Mr. Kidane's wiretapping and privacy claims are not actions for misrepresentation or deceit. Ethiopia lacks any persuasive means to attack that finding. Appellee's reliance on *JBP Acquisitions, LP v. U.S. ex rel. F.D.I.C.*, 224 F.3d 1260 (11th Cir. 2000) is off the mark. In *JBP Acquisitions*, the F.D.I.C. was alleged to have negotiated for the sale of a property it had already sold to the plaintiff JBP Acquisitions. *Id*. at 1262. That act was, at core, one of misrepresentation. The court held only that the FTCA exception for misrepresentation is triggered for "actions for negligence when the basis for the negligence action is an underlying claim for misrepresentation." *Id*. at 1264. This action is not based on "an underlying claim for misrepresentation." Indeed, this action would lie regardless of how Ethiopia managed to install its FinSpy malware on Mr. Kidane's computer

Consistent with this Court's holding in *Black v. Sheraton*, because Mr. Kidane does not base his tort claim on misrepresentations or deceitful conduct—but rather on the installation of computer spyware software and intentional interception, recording, and transmission of Mr. Kidane's private communications—Ethiopia's argument must be rejected.

V. THE WIRETAP ACT APPLIES TO FOREIGN SOVEREIGNS SUCH AS APPELLEE

Appellant's Opening Brief explains in detail the legal errors in the District Court's conclusion that § 2520(a) does not extend civil liability to government entities such as Ethiopia. Br. at 43-56.

In response, Appellee relies exclusively on the single Wiretap Act case finding that liability under § 2520(a) does not extend to government entities, *Seitz v. City of Elgin*, 719 F.3d 64, 658 (7th Cir. 2013). and fails to adequately address the rest. The additional cases cited in Appellee's footnote are inapposite as they do not address the Wiretap Act. Ethiopia cannot so easily skirt the plain language of section 2520.

The District Court conceded that the decision in *Seitz* goes against the weight of authority on this issue, noting that "many courts assume that the amendments to section 2520 covering governmental entities can be given meaning only if they are construed to have imposed a corresponding duty on governmental entities under section 2511(1) not to unlawfully intercept, endeavor to intercept, or procure another person to intercept communications. JA676. Indeed, the District Court's order cites at least eight other decisions that extended violations of section 2511(1) to government entities. *See* JA674, n.2. Still, the District Court disregarded that weight of authority to hold that the Wiretap Act does not apply to governmental entities such as Appellee.

Attempting to shore up the District Court's flawed analysis, Appellee notes that a *presumption* exists that "person" does not ordinarily include governmental entities, which can be overcome where there is an affirmative showing of statutory intent to the contrary. But Mr. Kidane does not contend that Ethiopia is a person. He contends that Ethiopia is an "entity" and that on the face of section 2520, an "entity" is civilly liable for violations of section 2511(1) that it "engaged in" through its agents. Since an entity can only engage in a tort through its agents, liability necessarily flows from agent to principal.

As fully explained in Appellant's Opening Brief, the text, structure, history, and purpose of the Wiretap Act all support the conclusion that civil liability under section 2520 was intended to attach to governmental entities for their agents' unlawful interceptions. And foreign states were not excepted from the law. Br. at 43-56. As Appellant's Opening Brief demonstrates, Congress was concerned with foreign states' ability to intercept electronic communications in the United States, when it enacted the Wiretap Act, yet it did not expressly carve them out of the statute's reach. Nor did it do so when it created an exception for the United States as part of USA PATRIOT Act. Thus both originally and upon amendment, the legislative history demonstrates that Congress did not create an exception for any governmental entities other than the United States for civil liability under the Wiretap Act.

VI. MR. KIDANE'S FIRST AMENDED COMPLAINT PROPERLY ALLEGES INTRUSION UPON SECLUSION

As an initial matter, Appellee's argument that Mr. Kidane's claim for intrusion upon seclusion is preempted by the Wiretap Act is an example of the Ethiopian government wanting to have its cake and eat it too. Indeed, Appellee's preemption argument is made just three pages later in its brief than its (erroneous) argument that the Wiretap Act does not apply at all to governmental entities. In other words, Ethiopia contends that it is simultaneously exempt from coverage under the Wiretap Act, but also insulated by its preclusive effect over State laws. As explained above and below, neither argument is correct.

To support its preemption argument, Ethiopia cites 18 U.S.C. § 2518(10). But this section of the Wiretap Act is limited in application to a motion "to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom . . . ." Thus, while section 2518(10)(c) does state that "[t]he remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications," it is simply inapplicable here. *See Leong v. Carrier IQ, Inc.*, 2012 U.S. Dist. LEXIS 59480, at *11 (C.D. Cal. Apr. 27, 2012). As the *Leong* court noted: "In this Court's view, [18 U.S.C. § 2518(10)(c)] does not even impact the question of preemption, but rather focuses on the scope of available federal

remedies when a violation of the statute has been established"; noting persuasive arguments that "a subsection of a provision addressing suppression of wiretap evidence obtained in violation of the Act, neither (1) explicitly provides for the preemption of state law; nor (2) applies outside the suppression context." *Id.* (citations omitted).

Furthermore, many federal courts have found that the Wiretap Act does *not* preempt more-restrictive state laws. For example, a federal court distinguished and criticized *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148 (C.D. Cal. 2007), that Ethiopia now cites, noting that federal laws establish minimum standards — without preempting the state law at issue.

Leong, 2012 U.S. Dist. LEXIS 59480, at *12–13; *see also Valentine v. Nebuad, Inc.*, 804 F. Supp. 2d 1022, 1029 (N.D. Cal. 2011) ("[t]he reasoning of *Bunnell* is unconvincing, however" since "[t]he quoted passage from the ECPA [18 U.S.C. § 2518(10)(c)] does not explicitly provide for the preemption of state law, which is the bar that must be met before express preemption may be found.").

But in any case, even if the Wiretap Act preempts Appellant's intrusion-upon-seclusion claim for the interception of his Skype internet telephone calls (and the District Court correctly held that it does not), Ethiopia makes no argument that it preempts the rest of Mr. Kidane's intrusion-upon-seclusion claim. Appellant's second cause of action is based on Ethiopia's monitoring of Mr. Kidane's private

computer usage, including web browsing and email usage. JA430-31, 451. Those activities are not alleged to be Wiretap Act violations and form an independent basis for liability that Ethiopia does not dispute.

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
Tel: (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) 474-9872

Counsel for Plaintiff-Appellant John Doe

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 28.1(e)(2) or 32(a)(7)(B) because:

   [X] this brief contains [*less than 7,000*] words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), *or*

   [ ] this brief uses a monospaced typeface and contains [*state the number of*] lines of text, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   [X] this brief has been prepared in a proportionally spaced typeface using [*Microsoft Word 2011*] in [*14pt Times New Roman*]; *or*

   [ ] this brief has been prepared in a monospaced typeface using [*state name and version of word processing program*] with [*state number of characters per inch and name of type style*].

Dated: December 27, 2016

/s/ *Richard M. Martinez*
Counsel for Appellant

CERTIFICATE OF FILING AND 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 REPLY 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 PHILLIP CHARROW
LAURA METCOFF KLAUS
THOMAS R. SNIDER
Greenberg Traurig, LLP
2101 L Street NW #1000
Washington, DC 20036

Counsel for Defendant-Appellee
Federal Democratic Republic of Ethiopia

MICHELLE RENEE BENNETT
U.S. Department of Justice
Civil Division
20 Massachusetts Avenue, NW
Room 7200
Washington, DC 20530

Counsel for interested party
United States of America

Dated: December 27, 2016

/s/ *Richard M. Martinez*
Counsel for Appellant

STATUTORY ADDENDUM

Except for the following, all applicable statutes, etc., are contained in either the Opening Brief for Appellant or the Brief for Appellee.

18 U.S.C. §2511

(1) Except as otherwise specifically provided in this chapter [18 USCS §§ 2510 et seq.] 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 [18 USCS §§ 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518], (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 [18 USCS §§ 2510 et seq.] 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 [50 USCS § 1801] 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 [50 USCS § 1881c] signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title [18 USCS § 2518(7)] 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 an order or certification under this subparagraph, 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 [18 USCS § 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 [18 USCS §§ 2510 et seq.].

(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 [18 USCS §§ 2510 et seq.] 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 [47 USCS §§ 151 et seq.] 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 [18 USCS §§ 2510 et seq.] 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 [18 USCS §§ 2510 et seq.] 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 [47 USCS § 605 or 606], 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 [50 USCS § 1801], as authorized by that Act [50 USCS §§ 1801 et seq.].

(f) Nothing contained in this chapter or chapter 121 or 206 of this title [18 USCS §§ 2510 et seq., or 2701 et seq., or 3121 et seq.], or section 705 of the Communications Act of 1934 [47 USCS § 605], 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 [50 USCS § 1801], and procedures in this chapter or chapter 121 or 206 of this title [18 USCS §§ 2510 et seq., or 2701 et seq., or 3121 et seq.] and the Foreign Intelligence Surveillance Act of 1978 [50 USCS §§ 1801 et seq.] shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act [50 USCS § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.] or chapter 121 of this title [18 USCS §§ 2701 et seq.] 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 [47 USCS § 553]; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 [47 USCS § 605(a)] by section 705(b) of that Act [47 USCS § 605(b)];

(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 [18 USCS §§ 2510 et seq.]--

(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) [18 USCS §§ 3121 et seq.]; 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 [18 USCS §§ 2510 et seq.] 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 [18 USCS § 2511(2)(a) or 2517];

(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 [18 USCS §§ 2510 et seq.] 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 [18 USCS §§ 2510 et seq.] 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 [18 USCS §§ 2510 et seq.] 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 [18 USCS § 2520], the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter [18 USCS §§ 2510 et seq.] 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 [18 USCS § 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.

18 U.S.C. §2520

(a) In general. Except as provided in section 2511(2)(a)(ii) [18 USCS § 2511(2)(a)(ii)], any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter [18 USCS §§ 2510 et seq.] may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief. In an action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages.

(1) In an action under this section, if the conduct in violation of this chapter [18 USCS §§ 2510 et seq.], is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is 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 is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) [18 USCS § 2511(5)] and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $ 50 and not more than $ 500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) [18 USCS § 2511(5)] or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual

damages suffered by the plaintiff, or statutory damages of not less than $ 100 and not more than $ 1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of--

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $ 100 a day for each day of violation or $ 10,000.

(d) Defense. A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title [18 USCS § 2518(7)]; or

(3) a good faith determination that section 2511(3) or 2511(2)(i) of this title [18 USCS § 2511(3) or 2511(2)(i)] permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter [18 USCS §§ 2510 et seq.] or any other law.

(e) Limitation. A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative discipline. If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter [18 USCS §§ 2510 et seq.], and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper disclosure is violation. Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 [18 USCS § 2517] is a violation of this chapter [18 USCS §§ 2510 et seq.] for purposes of section 2520(a) [18 USCS § 2520(a)].