THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JOHN DOE, a.k.a. KIDANE **Plaintiff,** **v.** **FEDERAL DEMOCRATIC, REPUBLIC OF ETHIOPIA** **Defendant.**	**Civil Action No. 1:14-cv-00372-CKK**

DEFENDANT'S MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED COMPLAINT
PURSUANT TO FEDERAL RULES 12(b)(1) and 12(b)(6)

Robert P. Charrow (DC 261958)
Thomas R. Snider (DC 477661)
GREENBERG TRAURIG, LLP
2101 L Street, N.W., Suite 1000
Washington, D.C. 20037
Tele: 202-533-2396; Fax: 202-261-0164
Email: charrowr@gtlaw.com;
snidert@gtlaw.com

Counsel for Defendant Federal Democratic Republic of Ethiopia

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

DEFENDANT'S MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED COMPLAINT PURSUANT TO FEDERAL RULES 12(b)(1) and 12(b)(6)

Introduction & Summary of Argument:

On June 27, 2014, the Federal Democratic Republic of Ethiopia ("Ethiopia") moved to dismiss Plaintiff's complaint under Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure. *See* Doc. # 20. Rather than responding to that motion, Plaintiff filed an amended complaint in an apparent effort to address a few of the many jurisdictional and other deficiencies in the original complaint by adroitly editing out admissions and adding adverbs. The amendments, if nothing else, highlight that this case ought to be dismissed for want of Article III jurisdiction.

This is a case about malware which, according Plaintiff, "tricked" him into accepting and opening an email from a friend and fooled his anti-virus programs, as well. As a result, the virus infected his home computer. Rather than chalking up his alleged computer infection to the work of criminals, who are doing it for profit, or hackers, who are doing it for sport, Plaintiff alleges instead that he is the victim of a conspiracy by Defendant to control his personal computer in Silver Spring, Maryland, from Ethiopia, even though he acknowledges that he was not the intended victim of the malware.

Plaintiff alleges that one of his friends received a threatening document via email, which Plaintiff assumes must have been sent by the Defendant from Ethiopia. *See* First Amended Complaint ("Amended Complaint" or "FAC") at ¶ 5. However, this "friend" is not named, his location is not revealed, and the complaint is devoid of any evidence that this email even came from Defendant. According to the anonymous Plaintiff, his anonymous friend, not the anonymous Plaintiff, was the target of the email and it was Plaintiff's anonymous friend who

forwarded the threatening document to Plaintiff. According to Plaintiff, the tainted document made its way into his friend's computer from another computer that used an Ethiopian routing address, and, from this, he infers that the Federal Democratic Republic of Ethiopia "controlled" the software and was responsible for its remote installation. These inferences cannot be justified as a matter of simple logic, given that computer addresses can be and are easily faked. *See* Cecilia Kang, *Fans know the score: No TVs needed*, WASH. POST, June 16, 2014, at A-1 (discussing how soccer fans use IP addresses from the UK to stream World Cup games for free, thereby avoiding pay-for-view cable).

The anonymous Plaintiff further alleges that, as a result of this computer virus, he has suffered statutory damages under the federal Wiretap Act and unspecified damages for "intrusion upon seclusion." As such, he instituted this suit against Ethiopia for declaratory relief and for money damages claiming that this Court has jurisdiction under 28 U.S.C. § 1330 by virtue of the so-called "tort" exception to the Foreign Sovereign Immunities Act ("FSIA"). *See* 28 U.S.C. § 1605(a)(5).[1] Simultaneously, Plaintiff, or those acting on his behalf, issued a press release and press statements about this suit, actions that are inconsistent with a plaintiff hoping to maintain low profile by filing suit anonymously. *See* Press Release, Electronic Frontier Foundation,

[1] Plaintiff also claims that this Court has jurisdiction under 28 U.S.C. §§ 1331 and 1367; further, he seeks declaratory relief and has demanded a jury trial. The Supreme Court and this Circuit have consistently held that the sole basis for jurisdiction against a sovereign, absent an international treaty to the contrary, is the FSIA which, under § 2(a), authorizes federal question jurisdiction exclusively under 28 U.S.C. § 1330; there is no other basis for federal jurisdiction. Therefore, sections 1331 and 1367 provide no jurisdictional basis for this action. Nor is a plaintiff entitled to a jury trial under the FSIA. Section 1330, the sole source of jurisdiction, permits only "nonjury civil actions." 28 U.S.C. § 1330(a); *see Wye Oak Tech., Inc. v. Republic of Iraq*, 941 F.Supp.2d 53, 61 (D.D.C. 2013); *Ruggiero v. Compania Peruana de Vapores "Inca Capac Yupanqui*," 639 F.2d 872, 875 (2d Cir. 1981) ("no jury can be had in an action in a federal court against a foreign state"). Finally, the only remedy available under the tort exception to the FSIA is money damages. There is no jurisdictional basis for declaratory relief. That form of relief is not authorized by section 1605(a)(5).

American Sues Ethiopian Government for Spyware Infection (Feb. 18, 2014), *available at* https://www.eff.org/press/releases/american-sues-ethiopian-government-spyware-infection.

Whether this is a serious litigation or one designed primarily as a press or political event is beside the point. In either case, this complaint must be dismissed in its entirety under Rule 12(b)(1) of the Federal Rules of Civil Procedure because the tort exception to sovereign immunity does not apply for five independent reasons.[2] First, under the law of this Circuit, the exception only applies if the entire tort "occurs in the United States." *Persinger v. Islamic Republic of Iran*, 729 F.2d 835, 842 (D.C. Cir.1984). This makes sense given that the exception was designed to provide Americans with a remedy should they be injured by a diplomat in a traffic accident in the United States. Here, according to Plaintiff, the tortious intent was formulated in Ethiopia and the acts took place in Ethiopia. The actors who committed the alleged tort, according to Plaintiff, were operating in Ethiopia, the computer servers were located in Ethiopia, the spyware was maintained in Ethiopia, the commands came from Ethiopia, and Plaintiff's materials were viewed in Ethiopia. Thus, the tort exception does not apply and, absent that exception, Ethiopia is immune from suit and this Court lacks subject matter jurisdiction. *See* 28 U.S.C. §§ 1330(a) & 1604.

Second, the tort exception, by its express terms, only applies to non-discretionary functions of a government. § 1605(a)(5)(A). Spying by a government, even if the allegations were true, is inherently a discretionary function and, therefore, not subject to a private civil action in a U.S. court.

---

[2] Defendant's counsel consulted with counsel for Plaintiff on August 1, 2014, to advise them of Defendant's intent to file a motion to dismiss under Rule 12(b) and to inquire whether they would dismiss this Complaint with prejudice. Plaintiff's counsel declined to dismiss this action.

Third, the tort exception, by its express terms, does not apply to any claim that arises as a result of a misrepresentation, deceit, or interference with contract. Spyware, such as the type alleged to have infected Plaintiff's computer, operates exclusively by tricking Plaintiff and his computer into believing that the document hosting the spyware is benign which then allows the virus to infect the machine. Both of Plaintiff's claims arise out of alleged deceit and thus, neither is actionable under the torts exception.

Fourth, the tort exception only applies if money damages are sought for "personal injury or death" or "damage to or loss of property." § 1605(a)(5). While Plaintiff alleges generically that he suffered "personal injury" (*see* FAC at ¶ 15), his claims for money damages are unrelated to any personal injury. In Count 1, he claims "statutory damages" under the Wiretap Act; he is not seeking damages for personal injury, as required by section 1605(a)(5). In Count 2, Plaintiff is claiming injury for "intrusion upon seclusion." This too is not a claim for "damages for personal injury."

Fifth, the complaint fails to state a claim for legally cognizable relief for any tort and, therefore, the tort exception does not apply. The interception provision of the Wiretap Act only applies to a "person," and the Act's definition of "person" does not include a foreign state. Moreover, the Wiretap Act does not even apply to the type of conduct at issue here. Nor is intrusion upon seclusion a viable claim. The FAC affirmatively claims that Defendant intended to invade the seclusion of another, not Plaintiff, and therefore, the requisite intent to invade Plaintiff's seclusion is absent. Moreover, the Wiretap Act expressly preempts common law claims such as "intrusion upon seclusion." *See* 18 U.S.C. § 2518(10)(c). Because of these shortcomings the complaint should also be dismissed under Rule 12(b)(6).

Summary of the Complaint:

Plaintiff, who is suing anonymously, [3] alleges that he is an Ethiopian-born citizen of the United States. *See* FAC at ¶ 3. He further alleges that Defendant "is a sovereign state located in East Africa" (*id*. at ¶ 21) and that, as alleged, it "seeks to undermine political opposition abroad." *Id.* at ¶ 24. According to the complaint, a European company--Gamma-- distributes a software product called "FinSpy," which can be used to infect computers by email. *See id.* at ¶¶ 28, 39. According to the Gamma website, it does not have offices in the United States. *See* https://www.gammagroup.com (last visited June 27, 2014). FinSpy is attached to an image or Word document, which serves as its Trojan Horse. It "attempt[s] to trick the victim into believing the opened file is not malicious." Exh. B at 8 (Doc. # 26 at 38). Once infected, the program, according to Plaintiff, allows an operator in a distant land access to the infected computer thereby enabling the overseas operator to read documents stored on the computer and to read emails that have already been sent or already been received, web searches that have already been conducted, and computer-based phone calls that have already taken place.

Plaintiff claims that an unnamed friend in an unnamed country received via email a document containing a "not-so-veiled threat against the [friend's] family." FAC at ¶ 56. Plaintiff then alleges "[o]n information and belief, [that] Defendant created the document . . . and intentionally infected the document with FinSpy." *Id*. Plaintiff's friend apparently forwarded the document to Plaintiff. *See id*. at ¶ 5.

After tricking Plaintiff into believing that the document was harmless, the spyware "then took what amounts to complete control over" Plaintiff's computer. *Id*. at ¶ 5; *see id*. at ¶ 41 and

[3] Should this matter proceed beyond this dispositive motion, Defendant reserves the right to ask this Court to permit Defendant's counsel access to the unredacted pleadings filed by Plaintiff thereby giving counsel access to Plaintiff's identify.

Exh. B at 8 (Doc. # 26 at 38). Plaintiff alleged that thereafter, the spyware began copying information, about his activities and those of his family, onto files in his computer and thereafter sent that information from those files to a server in Ethiopia. *See* FAC at ¶ 5. Plaintiff also alleges that "the FinSpy Master server in Ethiopia . . . is the same server that controlled the FinSpy target installation on [Plaintiff's] computer." *Id*. at ¶ 8 (emphasis added). The FAC goes on to allege that FinSpy "create[d] contemporaneous recording [on Plaintiff's computer] of his activities in Maryland, which the FinSpy programs then sent to the FinSpy Master server located in Ethiopia." *Id*. at ¶ 8 (emphasis supplied). Plaintiff alleges that "the FinSpy Relay and FinSpy Master servers with which Plaintiff's computer was controlled are located inside Ethiopia and controlled by Defendant Ethiopia." *Id*. at ¶ 85 (emphasis added).

Argument:

I. Ethiopia, As a Foreign Sovereign, Is Presumptively Immune From Suit

The FSIA "provides the sole basis for obtaining jurisdiction over a foreign state in the courts of this country." *Argentine Republic v. Amerada Hess Shipping Corp*., 488 U. S. 428, 443 (1989); *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1520 (D.C. Cir. 1984) (Scalia, J.), *cert. denied*, 470 U.S. 1051 (1985). Under the FSIA, a foreign state is presumptively immune from the jurisdiction of U.S. courts. Unless a specified exception applies, a federal court lacks subject-matter jurisdiction over a claim against a foreign state. *See Verlinden B. V. v. Central Bank of Nigeria*, 461 U. S. 480, 488-489 (1983); 28 U. S. C. § 1604; Joseph Dellapenna, SUING FOREIGN GOVERNMENTS AND THEIR CORPORATIONS 11, and n.64 (1988). Under the FSIA, the foreign sovereign has "immunity from trial and the attendant burdens of litigation . . . not just a defense to liability on the merits." *Phoenix Consulting, Inc. v. Republic of Angola*, 216 F.3d 36, 39 (D.C. Cir. 2000) (internal quotations and citations omitted).

Plaintiff bears the initial burden under the FSIA to show that a statutory exception to immunity applies. *See Cargill Int'l S.A. v. M/T Pavel Dybenko*, 991 F.2d 1012, 1016 (2d Cir. 1993). If none of the enumerated exceptions applies, then the Court lacks subject matter jurisdiction under 28 U.S.C. § 1330.

Plaintiff has invoked a single exception to sovereign immunity, the non-commercial tort exception which denies immunity in a case

> 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

28 U. S. C. § 1605(a)(5).

II. The Tort Exception Does Not Apply to the Allegations in the Amended Complaint

A. The Tort Exception Does Not Apply Where, As Here, the Entirety of the Alleged Tort Was Not Committed in the United States

Under the law of this Circuit, the "entirety of the tort must take place within the United States." *Von Dardel v. Union of Soviet Socialist Republics*, 736 F. Supp. 1, 7 (D.D.C. 1990); *see Asociacion de Reclamantes v. United Mexican States*, 735 F.2d at 1525 ("The tort, in whole, must occur in the United States") (quoting *In re Sedco, Inc*., 543 F. Supp. 561, 567 (S.D. Tex. 1982)); *Persinger v. Islamic Republic of Iran*, 729 F.2d 835, 842 (D.C. Cir.1984), *cert. denied*, 469 U.S. 881 (1984) (same): *Jerez v. Republic of Cuba*, 777 F.Supp.2d 6, 25 (D.D.C. 2011) (same); *see also O'Bryan v. Holy See*, 556 F.3d 361, 382 (6th Cir. 2009) (where the Sixth Circuit

"join[ed] the Second and D.C. Circuits in concluding that in order to apply the tortious act exception, the 'entire tort' must occur in the United States."); *Coleman v. Alcolac, Inc.,* 888 F.Supp. 1388, 1403 (S.D.Tex.1995) (exception not applicable because alleged tort "did not occur wholly in this country"); *Four Corners Helicopters, Inc. v. Turbomeca S.A.*, 677 F.Supp. 1096, 1102 (D. Col.1988) ("It is clear that in order for the exception to apply, the entire tort must have occurred in the United States"); *Antares Aircraft L.P. v. Federal Republic of Nigeria*, 1991 WL 29287 (S.D.N.Y. Mar. 1, 1991) ("It is well-recognized that for the non-commercial tort exception to apply, the entire tort must occur in the U.S.") (*aff'd on other grounds*, 948 F.2d 90 (2d Cir. 1991), *vacated mem.*, 505 U.S. 1215 (1992), *aff'd on other grounds*, 999 F.2d 33 (2d Cir. 1993)). Thus, only those torts which occurred entirely within the United States support jurisdiction under section 1605(a)(5).

This requirement follows from both the language of the FSIA and from *Amerada Hess Shipping* where the Court in holding that the "the exception in § 1605(a)(5) covers only torts occurring within the territorial jurisdiction of the United States," also noted that "Congress' primary purpose in enacting § 1605(a)(5) was to eliminate a foreign state's immunity for traffic accidents and other torts committed in the United States." 488 U.S. at 439-441. *See also* H. Rep. 94-1497, 94th Cong., 2d Sess. 20 (1976), 1976 U.S. CODE CONG. & AD. NEWS 6619 ("Section 1605(a)(5) is directed primarily at the problem of traffic accidents.").

Here, as alleged in the Amended Complaint, the acts underlying the tort, as distinct from their alleged injurious effect, occurred overseas, well outside the United States. The anonymous Plaintiff alleges that computers located in Ethiopia contained the main spyware programs and controlled his computer from Ethiopia. *See* FAC at ¶ 8 ("[T]he FinSpy Master server in Ethiopia disclosed in CitizenLab's report is the same server that controlled the FinSpy target installation

on Mr. Kidane's computer.") (emphasis added). The Amended Complaint goes on to allege that the FinSpy software "as well as infrastructure [are] run by the government operator of the system to collect the data." *Id*. at ¶ 31. The Amended Complaint also alleges that the computer "relay is located inside Ethiopia, and its operator is the Defendant in this action."[4] *Id*. at ¶ 60. Finally, Plaintiff alleges that "the FinSpy Relay and FinSpy Master servers with which Plaintiff's computer was controlled are located inside Ethiopia and controlled by Defendant Ethiopia." *Id.* at ¶ 85 (emphasis added).

Inasmuch as both the acts and intent occurred overseas, the two alleged intentional torts have their *situs* overseas and therefore, by definition did not occur entirely in the United States as required by the law of this Circuit. *See Darcars Motors of Silver Spring, Inc. v. Borzym*, 150 Md. App. 8, 818 A.2d 1159, 1169 (2003) (intentional tort consists of an act and the requisite and simultaneous intent); *In re Lett*, 238 B.R. 167, 183 (Bankr. W.D. Mo. 1999) (deceit-based intentional torts require temporal convergence of the *actus reus* and *mens rea*). The alleged act of remotely installing the software in Plaintiff's computer and control of that software and his computer all occurred allegedly in Ethiopia. Since the server and spyware were both located in Ethiopia, the information from Plaintiff's computer was transmitted to Ethiopia, the information was revealed to individuals located in Ethiopia, the human operators were located in Ethiopia and that any intent necessary to support the two alleged intentional torts had to have been

[4] It is difficult to understand how the FAC can possibly satisfy the requirements of section 1605(a)(5). Nations operate through their officers, officials and employees. Plaintiff has alleged that unidentified employees operated the computers in Ethiopia. There is no allegation that any of these officers or employees were acting within the scope of their office or employment as required by section 1605(a)(5). If no employee or officer is operating within the scope of their office or employment, it is difficult to understand how the sovereign can be held responsible under the FSIA or under any tort theory, statutory or otherwise.

formulated in Ethiopia, the *situs* of these alleged torts was Ethiopia. As such, they were not entirely within the United States.

Nothing in the Amended Complaint suggests otherwise. Plaintiff, having had the benefit of a sneak preview of Defendant's motion to dismiss, added some adverbs to the original complaint in an effort to address the requirement that entire tort must take place in the United States. Thus, by way of example, rather than stating, as he did in the original complaint, that Defendant "caused personal injury to Plaintiff" (Complaint at ¶ 15), Plaintiff now pleads in his FAC that the Defendant "caused personal injury to Plaintiff . . . entirely at Plaintiff's residence in Silver Spring, Maryland." FAC at ¶ 15 (emphasis supplied). The fact that the entire alleged injury may have occurred in Maryland is not relevant; it is the *situs* of the tort that counts and here, all defendant's actions were alleged to have taken place overseas: the computers that controlled plaintiff's computer, according to the FAC, "are located inside Ethiopia and controlled by Defendant Ethiopia." FAC ¶ 85.

In that regard, *O'Bryan v. Holy See* is instructive and dispositive. There plaintiffs, who claimed to have been victims of sexual abuse by Roman Catholic clergy, filed a class action suit against the Holy See, alleging, among other things, that the Holy See negligently failed to warn them of the dangers, negligently supervised its clergy, and affirmatively covered-up the actions of its errant clergy. These acts or omissions all took place in Vatican City, but had their effect in the United States where they caused the plaintiffs' injuries. In dismissing the tort claims against the Holy See for its conduct, as opposed to the tortious conduct of its U.S. employees in the United States, the Court concluded that

> any portion of plaintiffs' claims that relies upon acts committed by the Holy See abroad cannot survive. For example, the tortious act exception to the FSIA's grant of immunity would not include any theory of liability premised on the Holy See's own negligent supervision because such acts presumably occurred abroad; moreover, a direct claim

> leveled against the Holy See for promulgating the 1962 Policy [cover-up policy] would not fall within the tortious act exception because it too presumably occurred abroad. In turn, plaintiffs cannot pursue claims based upon the alleged sexual abuse of priests or based upon the acts of the Holy See that occurred abroad.

O'Bryan v. Holy See, 556 F.3d at 385-86.

This case is no different. Since the alleged tort and the alleged tortfeasors were allegedly located in and operated in Ethiopia, the entire tort was not alleged to have taken place in the United States, as required under the law of this Circuit. As such, the tort exception does not apply; Ethiopia retains immunity and this Court lacks jurisdiction under section 1330.

B. The Tort Exception Does Not Apply to the Discretionary Functions Alleged in the Amended Complaint

By its terms, the tort exception does "not apply to [ ] 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." 28 U.S.C. § 1605(a)(5)(A). "This exemption was modeled on the discretionary function exemption to the [Federal Tort Claims Act], 28 U.S.C. § 2680(a), House Report, *supra*, at [21, 1976 U.S. CODE CONG. & AD. NEWS] 6620, and cases construing the FTCA are therefore applicable here, *Sheldon ex rel. Olsen v. Government of Mexico*, 729 F.2d 641, 646-47 (9th Cir.), *cert. denied*, 469 U.S. 917 (1984)." *De Sanchez v. Banco Central De Nicaragua*, 770 F.2d 1385, 1399 n.19 (5th Cir. 1985). Under the exemption, governments are not liable "[w]here there is room for policy judgment." *Dalehite v. United States*, 346 U.S. 15, 36 (1953). The Court construed the discretionary function provision of the FTCA as intending to preserve immunity for "decisions grounded in social, economic, and political policy." *United States v. S.A. Empresa De Viacao Aerea Rio Grandense (Varig Airlines),* 467 U.S. 797, 814 (1984). The Court also directed that it is "the nature of the conduct, rather than the

status of the actor, that governs whether the discretionary function exception applies in a given case." *Id*. at 813.

Courts use a two-step analysis to determine whether challenged conduct falls under the discretionary function exception. First, one determines whether the challenged actions involve "an element of judgment or choice." *United States v. Gaubert*, 499 U.S. 315, 322 (1991) (quotation omitted). If the challenged actions involve an element of choice or judgment, a court must determine "whether that judgment is of the kind that the discretionary function exception was designed to shield." *Gaubert*, 499 U.S. at 322-23. More specifically, if the judgment involves considerations of social, economic, or political policy, the exception applies. *See Varig Airlines*, 467 U.S. at 814; *MacArthur Area Citizens Ass'n v. Republic of Peru*, 809 F.2d 918, 922 *modified on other grounds*, 823 F.2d 606 (D.C. Cir. 1987).

The decisions by intelligence services, both foreign and domestic, on who will be placed under surveillance or will be spied upon and how, by definition, involve an element of choice. The alleged decisions are also quintessentially political in nature, a fact acknowledged by Plaintiff when he argues that the decision to target specific individuals was "politically motivated." *See* FAC at ¶¶ 22-25; Exh. B at 1 (Doc. #26 at 31). As such, the alleged activities are, by definition, discretionary functions within the meaning of the FSIA and FTCA. This is especially so here, where Plaintiff has acknowledged working for the group Ginbot 7, "some of whose members," according to the U.S. State Department, "publicly advocated violent overthrow of the government." *See* Declaration of John Doe (AKA "Kidane") in Support of Motion for Leave to Proceed in Pseudonym (Doc. 1-1,"Declaration") at ¶ 9; <http://www.state.gov/j/drl/rls/hrrpt/2010/af/154346.htm> (last visited July 29, 2014).

In *Burnett v. Al Baraka Invest. and Dev. Corp*., 292 F.Supp.2d 9 (D.D.C. 2003), plaintiffs alleged that the director of Saudi Arabia's intelligence service authorized funding for certain organizations, some of which ultimately participated in the 9/11 attack. The Court concluded that decisions by foreign governments on who to fund and how to fund were inherently discretionary functions and not subject to the tort exception of the FSIA. *See id*. at 20 ("[T]he official acts plaintiffs ascribe to Prince Turki and Prince Sultan are squarely covered by the 'discretionary function' language of subsection A [of § 1605(a)(5)]."). Correspondingly, in *Jin v. Ministry of State Security*, 475 F.Supp.2d 54, 67 (D.D.C. 2007), plaintiffs, a religious minority in China, instituted suit against the Chinese Ministry of State Security and others for harassing and threatening them in the United States. In dismissing the tort claims, the Court concluded that the actions of the Chinese government were discretionary, especially defendants' "decisions regarding its thugs [hired to injure and intimidate members of the Falun Gong in the United States] *e.g*., hiring, training, and supervising … clearly 'involve a measure of policy judgment.'" Since the actions were discretionary functions, the tort exception to sovereign immunity did not apply. *See also Bruce v. Consulate of Venezuela*, No. 04-933 (RWR) (D.D.C. Aug. 31, 2005) (holding that defendant consulate exercised a discretionary function by including plaintiff's name in a letter even though that letter was alleged to have invaded plaintiff's privacy); *Risk v. Halvorsen*, 936 F.2d 393 (9th Cir. 1991) (diplomat aiding Norwegian citizen in returning to Norway with her children in violation of state court custody order was a discretionary function).

C. The Tort Exception Does Not Apply to Claims Based on Deceit, as Alleged in the Amended Complaint

Section 1605(a)(5)(B) bars "any claim arising out of . . . misrepresentation, deceit, or interference with contract rights." *See TIFA, Ltd. v. Republic of Ghana*, CIV.A . 88-1513, 1991 WL 179098 (D.D.C. Aug. 27, 1991) ("The clear language of subsection 1605(a)(5)(B) bars suits

for misrepresentation or deceit."). Here, both claims in the FAC necessarily arise out of alleged deceitful conduct. The purpose of FinSpy, as Plaintiff alleges, is to "trick" the Plaintiff "into opening" an infected file. FAC ¶ 41 (emphasis supplied). "The target is therefore unaware that his computer has been infected." *Id*. According to Plaintiff, FinSpy, as employed by defendant, "attempt[s] to trick the victim into believing the opened file is not malicious." Doc. # 26 at 38 (emphasis supplied). Trickery, though, is nothing more than "deceit" or "misrepresentation." *See* BLACK'S LAW DICTIONARY 405 (6th ed. 1990). The FSIA, though, bars such suits.

D. The Tort Exception Does Not Apply to Statutory Damages or to Injuries for Annoyance, as Alleged in the Amended Complaint

The tort exception, as relevant here, only applies to claims for money damages "for personal injury or death." Exceptions to sovereign immunity are strictly construed. *F.A.A. v. Cooper*, 566 U.S. ___, 132 S. Ct. 1441, 1448 (2012); *Lane v. Pena*, 518 U.S. 187, 192 (1996); *see also Haven v. Polska,* 215 F.3d 727, 731 (7th Cir. 2000) (noting that FSIA exceptions must be "narrowly construed" because they are "in derogation of the common law"). Here, Plaintiff "seeks statutory damages under the Wiretap Act." FAC at ¶ 12.

The FSIA's tort exception, however, does not authorize a plaintiff to seek statutory damages from a sovereign; it only authorizes recovery of damages for personal injury. Statutory damages are used when plaintiff is unlikely to have suffered any real damage, but Congress nonetheless strives to discourage the defendant's conduct. *See* S. Rep. No. 94-938, 94th Cong., 2d Sess. 348 (1976) ("Because of the difficulty in establishing in monetary terms the damages sustained by a taxpayer as the result of the invasion of his privacy caused by an unlawful disclosure of his returns or return information, [26 U. S. C. § 7217(c)] provides that these damages would, in no event, be less than liquidated damages of $1,000 for each disclosure.");

but see Doe v. Chao, 540 U.S. 614 (2004) (statutory damages are not available under the Privacy Act unless plaintiff proves actual damages).

Correspondingly, under the common law tort of "intrusion upon seclusion," one may recover damages for "harm to his interest in privacy resulting from the invasion," as well as damages for "mental distress." RESTATEMENT (SECOND) OF TORTS § 652H (1977). In his original complaint, Plaintiff did not allege that he has suffered any "mental" or "emotional distress." After reviewing the original Memorandum in Support of Ethiopia's Motion to Dismiss, where this failing was noted, Plaintiff has suddenly become the sufferer of emotional distress. *See* FAC at ¶ 91. It is mentioned once in the Amended Complaint.

Here, though, "emotional distress" is jurisdictional. As such, Plaintiff has to do more than merely make a bald assertion that he suffered personal injury or emotional distress. *See Ashcroft v. Iqbal*, 556 U.S. 662 (2009); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007). This is especially the case where both the statute and common law tort recognize the unlikelihood that a plaintiff would suffer actual "personal injury" as a result of the invasion. *See* RESTATEMENT § 652H, cmt. c (noting that "[w]hether in the absence of proof of actual harm an action might be maintained for nominal damages remains uncertain"). Plaintiff's belated assertion of emotional distress rings hollow.

E. The Tort Exception Does Not Apply to Either Violations of the Wiretap Act or Common Law "Intrusion Upon Seclusion"

1. The Amended Complaint Does Not Allege a Violation of the Wiretap Act

a. The Interception Provision of the Wiretap Act Does Not Apply to Sovereigns

Under the Wiretap Act, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter 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." 18 U.S.C. § 2520(a) (emphasis supplied). Here, the anonymous Plaintiff alleges that Defendant violated section 2511 "by [the] unlawful interception of Plaintiff's communications." FAC at ¶¶ 15 and 91. No other provisions of the Wiretap Act are referenced in the Complaint. The "interception" provision of section 2511(1) reads as follows:

> 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;

Thus, by its terms, only a "person" can violate section 2511(1). The Wiretap Act, though, defines "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[.]" *Id.* at § 2510(6). As so defined, the term "person" excludes foreign sovereigns, at least with respect to the Act's interception provisions. This is consistent with the "longstanding interpretive presumption that 'person' does not include the sovereign." *Vermont Agency of Natural Res. v. United States ex rel. Stevens*, 529 U.S. 765, 780-81 (2000); *see also Price v. Socialist People's Libyan Arab Jamahiriya*, 294 F.3d 82, 96 (D.C. Cir. 2002) ("[W]e hold that foreign states are not 'persons' protected by the Fifth Amendment."). [5] Here, the presumption is conclusive. The definition of person includes certain sovereigns, such as the

[5] If this Court were to hold that "person" includes a foreign state, then that meaning should also apply to all due process considerations, and this motion should also be construed as a motion to dismiss under Rule 12(b)(2) for lack of minimum contacts and hence lack of personal jurisdiction, notwithstanding section 1330. Plaintiff has not alleged minimum contacts under the Due Process Clause sufficient to support personal jurisdiction.

domestic States, but does not include the United States or foreign states, both of which are mentioned elsewhere in the statute. *See, e.g.*, 18 U.S.C. §§ 2510(19), 2517(6), 2517(8).

Given that the "interception" provision of the Wiretap Act does not apply to foreign sovereigns, Plaintiff has failed not only to state a claim upon which relief can be granted for Rule 12(b)(6) purposes, but also has failed to plead a statutory tort necessary to support the tort exception to Ethiopia's sovereign immunity for Rule 12(b)(1) purposes.

b. The Amended Complaint Fails to Allege a Necessary "Interception" to Support a Wiretap Act Claim

The activities hypothesized in the Amended Complaint do not even give rise to a civil cause of action under the Wiretap Act. Plaintiff claims that Defendant violated the "interception" provision of the Act. *See, e.g.*, FAC at ¶ 87 ("On information and belief, the FinSpy software used the downloaded modules to *automatically* intercept Plaintiff's *private* communications, resulting in a contemporaneous interception of Plaintiff's communication on his computer in Maryland" on Defendant Ethiopia's instruction). To make a claim under the Wiretap Act, plaintiff must plead that a defendant (1) intentionally (2) intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device.

"Interception" is defined 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). "The Circuits which have interpreted this definition as applied to electronic communications have held that it encompasses only acquisitions contemporaneous with transmission." *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir.), *cert. denied*, 538 U.S. 1051 (2003) (collecting cases from Fifth and Ninth Circuits) (emphasis supplied). *See Theofel v. Farey–Jones*, 359 F.3d 1066, 1077–78 (9th Cir. 2004) (post-delivery); *Fraser v.*

Nationwide Mut. Ins. Co., 352 F.3d 107, 113–14 (3d Cir. 2003) (post-delivery); *Konop v. Hawaiian Airlines*, 302 F.3d 868, 878–79 (9th Cir. 2002) (on website server), *cert. denied*, 537 U.S. 1193 (2003); *Steve Jackson Games, Inc. v. United States Secret Serv*., 36 F.3d 457, 461–62 (5th Cir. 1994) (pre-retrieval); *but see United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (en banc) (holding that an interception under ECPA does not require contemporaneous access).

Thus, in *Steiger* the court held that the use of a virus to access and download information stored on a personal computer did not constitute an interception of electronic communications in violation of the Wiretap Act because the record did not "suggest that any of the information provided in the . . . emails . . . was obtained through contemporaneous acquisition of electronic communications while in flight." *Steiger*, 318 F.3d at 1050. This mirrors precisely the allegations in the original Complaint and in the Amended Complaint, notwithstanding Plaintiff's liberal insertion of the words "contemporaneous" or "contemporaneously" throughout the Amended Complaint.

In the original Motion to Dismiss, Defendant noted that the Complaint contained "no allegation that the defendant acquired any information contemporaneously with its communication." To the contrary, the Complaint was replete with allegations that the virus placed information into temporary folders for subsequent transmission by defendant. In short, acquisition and transmission did not occur contemporaneously as required, and, therefore, Plaintiff had not pled a violation of the Wiretap Act.

In effort to address this shortcoming, Plaintiff added the word "contemporaneous" or its adverbial variant, "contemporaneously," a total of nine times in the FAC. The addition of an adjective or adverb does not and cannot alter the underlying facts, which remain unchanged in

the FAC. Plaintiff now alleges, for instance, that telephone conversations and email transmissions are "contemporaneous[ly] record[ed]" on his computer and then later transmitted to Ethiopia. FAC at ¶ 10 ("FinSpy programs installed on the Kidane family computer in Maryland to create contemporaneous recording of his activities in Maryland, which the FinSpy programs then sent to the FinSpy Master server located in Ethiopia."); *id*. at ¶ 37 ("FinSpy also contains a module for the contemporaneous recording of Internet telephone calls, text messages, and file transfers"); *id.* at ¶ 48 ("In some cases, such as the case of the FinSpy Skype module, the module first contemporaneously intercepts and copies the data, unencrypted, to files on the infected computer's temporary folder on its hard disk."). However, to constitute an "interception," the transmission to the eavesdropper must occur at the time the conversation or communication is taking place; the interception must be in real time. That is not the case here. Rather, here like in *Steiger,* the information is first recorded by the malware onto the Plaintiff's own computer and then later transmitted abroad. That is what Plaintiff originally alleged, and aside from some adroit editing, that is still what is being alleged. The allegations were legally inadequate when originally lodged and the amendments have not remedied that.

2. Plaintiff Has Not and Cannot Plead Intrusion Upon Seclusion

(a) The Amended Complaint Does Not Allege that Defendant Intentionally Intruded on Plaintiff's Seclusion

The tort known as "intrusion upon seclusion" is committed when

> [o]ne who *intentionally* intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Bailer v. Erie Ins. Exch., 344 Md. 515, 526, 687 A.2d 1375, 1380-81 (1997) (emphasis in original).

"The tort cannot be committed by unintended conduct amounting merely to lack of due care. Intentional conduct is a necessary element of the cause of action." *Id*. The "intrusion" must be intentional. Here, the alleged intrusion occurred when Plaintiff was tricked into opening a document that one of his friends had forwarded to him. This document, which allegedly contained spyware, was not addressed to Plaintiff and there is no allegation that Defendant mailed or sent the document to Plaintiff. Nor is there any allegation that Plaintiff was the intended target of the email carrying the alleged spyware. To the contrary, even as hypothesized by Plaintiff, Plaintiff was not the intended target; his unidentified friend may have been the intended target, but that friend is not a party to this suit. In short, there is no allegation that Defendant intended to invade Plaintiff's seclusion and therefore, Plaintiff has failed to plead a claim for which relief can be granted.

(b) Common Law Torts, Such as Intrusion Upon Seclusion, Are Expressly Preempted by the Wiretap Act

Plaintiff has failed to state claim for intrusion upon seclusion for a second reason: the Wiretap Act expressly preempts any state common law claim for relief, as follows:

> The 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."

18 U.S.C. § 2518(10)(c); *see Bunnell v. Motion Picture Ass'n of America*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007); *see also Quon v. Arch Wireless Operating Co., Inc.*, 445 F. Supp. 2d 1116, 1138 (C.D. Cal. 2006) *aff'd in part, rev'd in part on unrelated grounds*, 529 F.3d 892 (9th Cir. 2008) *rev'd and remanded sub nom. City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010) (holding 18 U.S.C. § 2708, which states that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this

chapter" preempted state law claims of invasion of privacy). [6] Accordingly, Plaintiff's tort claim for intrusion upon seclusion is preempted by the Wiretap Act.

Conclusion:

For the foregoing reasons, Defendant's Motion to Dismiss for want of subject matter jurisdiction under the Foreign Sovereign Immunities Act and for failure state to a claim should be granted and Plaintiff's First Amended Complaint should be dismissed with prejudice.

Dated: August 4, 2014

Respectfully submitted,

/s/ Robert P. Charrow

Robert P. Charrow (DC 261958)
Thomas R. Snider (DC 477661)
GREENBERG TRAURIG, LLP
2101 L Street, N.W., Suite 1000
Washington, D.C. 20037
Tele: 202-533-2396; Fax: 202-261-0164
Email: charrowr@gtlaw.com;
snidert@gtlaw.com

Counsel for Defendant Federal Democratic Republic of Ethiopia

[6] Some courts have held that the Wiretap Act does not preempt state law because the Act only sets minimum standards for the protection of privacy, leaving the states free to provide remedies beyond those provided for by the Wiretap Act. *See, e.g.*, *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022, 1029 (N.D. Cal. 2011); *Lane v. CBS Broadcasting Inc.*, 612 F. Supp. 2d 623 (E.D. Pa. 2009). However, those courts did not address the Article III implications of their holdings. Under Article III, a plaintiff must plead and prove that he or she has standing by showing, among other things, that the court can remedy the alleged injury. *Lujan v. Defenders of Wildlife*, 504 US 555, 561 (1992). In the present case, the statute precludes a court from providing any remedy beyond that which is provided by the Wiretap Act. Therefore, plaintiff lacks Article III standing to pursue any claim other than a claim under the Wiretap Act. *See City of Los Angeles v. Lyons*, 461 U.S. 95 (1983) (holding that standing is a claim by claim, remedy by remedy undertaking).