

**THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

---

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

---

**DEFENDANT’S MOTION TO DISMISS  
PURSUANT TO FEDERAL RULES 12(b)(1) and 12(b)(6)**

Pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, Defendant Federal Democratic Republic of Ethiopia (“Ethiopia”) hereby moves this Court to dismiss Plaintiff John Doe, a.k.a. Kidane’s (“Plaintiff”) complaint (Docket No. 3). As set forth in the accompanying Memorandum, this Court lacks subject matter jurisdiction because Ethiopia is a foreign sovereign, which, under the Foreign Sovereign Immunities Act (“FSIA”), is immune from suit, unless Plaintiff can demonstrate that the suit falls within a specified statutory exception to immunity. Here, the sole exception – the “tort” exception – on which Plaintiff relies, does not apply. Accordingly, Ethiopia retains its immunity and this Court lacks subject matter jurisdiction.

Plaintiff also has failed to state a legally-cognizable claim and, therefore, his complaint is also subject to dismissal under Federal Rule 12(b)(6).

WHEREFORE, for these reasons, as well as those set forth in the accompanying memorandum, Ethiopia respectfully requests that the Court dismiss Plaintiff's complaint.<sup>1</sup>

Dated: June 27, 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

Tel: 202-533-2396; Fax: 202-261-0164

Email: charrowr@gtlaw.com;

snidert@gtlaw.com

Counsel for Defendant Federal Democratic  
Republic of Ethiopia

---

<sup>1</sup> By filing this motion, accompanying memorandum, and proposed order, Ethiopia is not waiving its sovereign immunity.



**TABLE OF CONTENTS**

TABLE OF AUTHORITIES ..... ii

INTRODUCTION AND SUMMARY OF ARGUMENT ..... 1

SUMMARY OF THE COMPLAINT ..... 4

ARGUMENT ..... 5

I. ETHIOPIA, AS A FOREIGN SOVEREIGN, IS PRESUMPTIVELY IMMUNE FROM  
SUIT ..... 5

II. THE TORT EXCEPTION DOES NOT APPLY TO THE ALLEGATIONS IN THE  
COMPLAINT ..... 6

    A. The Tort Exception Does Not Apply Where, As Here, the Entirety of the Alleged  
    Tort was not Committed in the United States. .... 6

    B. The Tort Exception Does Not Apply to the Discretionary Functions Alleged in  
    this Complaint ..... 8

    C. The Tort Exception Does Not Apply to Statutory Damages or to Injuries for  
    Annoyance, as Alleged in this Complaint ..... 10

    D. The Torts Exception Does not Apply to Either Violations of the Wiretap Act or  
    Common Law “Intrusion Upon Seclusion” ..... 11

        1. Pleadings Do Not Allege a Violation of the Wiretap Act ..... 11

            a. The Interception Provision of the Wiretap Act Does Not Apply  
            to Sovereigns ..... 11

            b. Complaint Fails to Allege a Necessary “Interception” to Support  
            a Wiretap Act Claim. .... 13

        2. Common Law Torts, Such as Intrusion Upon Seclusion, Are Expressly  
        Preempted by the Wiretap Act ..... 14

CONCLUSION ..... 15

**TABLE OF AUTHORITIES**

**Cases**

*Argentine Republic v. Amerada Hess Shipping Corp.*,  
488 U. S. 428 (1989).....5,6,7

*Ashcroft v. Iqbal*,  
556 U.S. 662 (2009).....11

*Asociacion de Reclamantes v. United Mexican States*,  
735 F.2d 1517 (D.C. Cir. 1984).....5,6

*Bell Atlantic Corp. v. Twombly*,  
550 U.S. 544 (2007).....11

*Brzak v. United Nations*,  
597 F.3d 107 (3d Cir. 2010).....2

*Bruce v. Consulate of Venezuela*,  
No. 04-933 (RWR) (D.D.C. Aug. 31, 2005).....10

*Bunnell v. Motion Picture Ass’n of America*,  
567 F. Supp. 2d 1148 (C.D. Cal. 2007) .....14

*Burnett v. Al Baraka Invest. and Dev. Corp.*,  
292 F.Supp.2d 9 (D.D.C. 2003).....9

*Cargill Int’l S.A. v. M/T Pavel Dybenko*,  
991 F.2d 1012 (2d Cir. 1993).....5

*City of Ontario, Cal. v. Quon*,  
560 U.S. 746 (2010).....14

*City of Los Angeles v. Lyons*,  
461 U.S. 95 (1983).....15

*Dalehite v. United States*,  
346 U.S. 15 (1953).....8

*De Sanchez v. Banco Central De Nicaragua*,  
770 F.2d 1385 (5th Cir. 1985). .....8

*Doe v. Chao*,  
540. U.S. 614 (2004).....10

*F.A.A. v. Cooper*,  
566 U.S. \_\_\_, 132 S. Ct. 1441 (2012).....11

*Fraser v. Nationwide Mut. Ins. Co.*,  
352 F.3d 107 (3d Cir. 2003).....13

*Jerez v. Republic of Cuba*,  
777 F.Supp.2d 6 (D.D.C. 2011).....6

*Jin v. Ministry of State Security*,  
475 F.Supp.2d 54 (D.D.C. 2007).....9

*Kiobel v. Royal Dutch Petroleum Co.*,  
\_\_\_ U.S. \_\_\_, 133 S.Ct. 1659 (2013).....7

*Konop v. Hawaiian Airlines*,  
302 F.3d 868 (9th Cir. 2002). ....13

*Lane v. CBS Broadcasting Inc.*,  
612 F. Supp. 2d 623 (E.D. Pa. 2009).....15

*Lane v. Pena*,  
518 U.S. 187 (1996).....10

*Lujan v. Defenders of Wildlife*,  
504 U.S. 555 (1992).....15

*MacArthur Area Citizens Ass'n v. Republic of Peru*,  
809 F.2d 918 (D.C. Cir. 1987).....9

*O’Bryan v. Holy See*,  
556 F.3d 361 (6th Cir. 2009). ....6

*Persinger v. Islamic Republic of Iran*,  
729 F.2d 835 (D.C. Cir. 1984).....2,6

*Phoenix Consulting, Inc. v. Republic of Angola*,  
216 F.3d 36 (D.C. Cir. 2000).....5

*Price v. Socialist People’s Libyan Arab Jamahiriya*,  
294 F.3d 82 (D.C. Cir. 2002).....12

*Quon v. Arch Wireless Operating Co., Inc.*,  
445 F. Supp. 2d 1116 (C.D. Cal. 2006) .....14

*Risk v. Halvorsen*,  
936 F.2d 393 (9th Cir. 1991). .....10

*Sheldon ex rel. Olsen v. Government of Mexico*,  
729 F.2d 641 (9th Cir.). .....8

*State v. Williams*,  
94 Wash. 2d 531 (1980). .....15

*Steve Jackson Games, Inc. v. United States Secret Serv.*,  
36 F.3d 457 (5th Cir. 1994) .....13

*Theofel v. Farey–Jones*,  
359 F.3d 1066 (9th Cir. 2004). .....13

*United States v. Councilman*,  
418 F.3d 67 (1st Cir. 2005). .....14

*United States v. Gaubert*,  
499 U.S. 315, 322 (1991). .....9

*United States v. S.A. Empresa De Viacao Aerea Rio Grandense (Varig Airlines)*,  
467 U.S. 797 (1984). .....8

*United States v. Steiger*,  
318 F.3d 1039 (11th Cir.). .....13,14

*Valentine v. NebuAd, Inc.*,  
804 F. Supp. 2d 1022 (N.D. Cal. 2011). .....15

*Verlinden B. V. v. Central Bank of Nigeria*,  
461 U. S. 480 (1983). .....5

*Vermont Agency of Natural Res. v. United States ex rel. Stevens*,  
529 U.S. 765 (2000). .....12

*Von Dardel v. Union of Soviet Socialist Republics*,  
736 F. Supp. 1 (D.D.C. 1990). .....6

*Wye Oak Tech., Inc. v. Republic of Iraq*,  
941 F.Supp.2d 53 (D.D.C. 2013). .....2

Statutes  
18 U.S.C. § 2510. ....12,13

18 U.S.C. § 2511.....12

18 U.S.C. § 2517.....12

18 U.S.C. § 2518.....4,14

18 U.S.C. § 2520(a).....12

28 U.S.C. § 1330 .....2,3,6,8,12

28 U.S.C. § 1331.....2

28 U.S.C. § 1367.....2

28 U.S.C. § 1604.....3,5

28 U.S.C. § 1605(a) .....2,3,6,7,8,9

28 U.S.C. § 2680(a) .....8

Rules

Fed. R. Civ. P. 12(b)(1).....2,13

Fed. R. Civ. P. 12(b)(2).....12

Fed. R. Civ. P. 12(b)(6).....4,13

Other Authorities

Press Release, Electronic Frontier Foundation, American Sues Ethiopian Government for  
Spyware Infection (Feb. 18, 2004). .....2

Cecilia Kang, *Fans know the score: No TVs needed*,  
The Washington Post, June 16, 2014.....1

Joseph Dellapenna, *Suing Foreign Governments and Their Corporations*,  
1<sup>st</sup> ed., The Bureau of National Affairs: Washington, D.C. (1988). .....5

Stefan Saroiu, Steven D. Gribble, and Henry M. Levy, *Measurement and Analysis of Spyware in  
a University Environment*, 1 Networked Sys. Design & Implementation (March 2004).....1

S. Comm. Homeland Sec. and Governmental Aff. Permanent Subcomm. Investigations,  
Report on Online Advertising and Hidden Hazards to Consumer Security and Data  
Privacy (2014).....1



S. Rep. No. 94-938 (1976).....	10
RESTATEMENT (SECOND) OF TORTS (1977).....	11

**DEFENDANT’S MEMORANDUM IN SUPPORT OF ITS MOTION TO DISMISS  
PURSUANT TO FEDERAL RULES 12(b)(1) and 12(b)(6)**

**Introduction & Summary of Argument:**

Malware and spyware infect tens of millions of computers annually, and like the common cold, they draw little distinction between the big and small, or the rich and poor; they infect a full range of devices from mega-servers owned by giant corporations, such as Target, to personal computers owned by individuals, such as Plaintiff, according to the allegations in the Complaint.<sup>1</sup> Rather than chalking up his computer virus 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 to infect and control his personal computer in Silver Spring, Maryland, from Ethiopia.

Plaintiff alleges that his computer in Maryland was hacked with software purchased abroad from a European company, that some of this software made its way into his computer through another computer that used an Ethiopian routing address, and, from this, he infers that the Federal Democratic Republic of Ethiopia (“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

---

<sup>1</sup> *See* S. Comm. Homeland Sec. and Governmental Aff. Permanent Subcomm. Investigations, 113th Cong., Rep. on Online Advertising And Hidden Hazards To Consumer Security And Data Privacy (2014), *available at* <http://www.hsgac.senate.gov/hearings/online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy>; Stefan Saroiu, Steven D. Gribble, and Henry M. Levy, *Measurement and Analysis of Spyware in a University Environment*, 1 NETWORKED SYS. DESIGN & IMPLEMENTATION (Mar. 2004).

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).<sup>2</sup> 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 a low profile by filing suit anonymously. *See* Press Release, Electronic Frontier Foundation, 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 four independent reasons.<sup>3</sup> 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

---

<sup>2</sup> 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. *See Wye Oak Tech., Inc. v. Republic of Iraq*, 941 F.Supp.2d 53, 61 (D.D.C. 2013); *Brzak v. United Nations*, 597 F.3d 107 (3d Cir. 2010) (rejecting a Seventh Amendment challenge to the FSIA). 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).

<sup>3</sup> Defendant’s counsel consulted with counsel for Plaintiff on June 26, 2014, advising them of Defendant’s intent to file a motion to dismiss under Rule 12(b) and inquiring whether they would dismiss this Complaint. Plaintiff’s counsel indicated that they would not.

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 intent was formulated 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 in Ethiopia, the commands came from Ethiopia, and the software was 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.

Third, 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* Complaint 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. The Wiretap Act does not provide a private right of action for “personal injury,” as required by section 1605(a)(5). In Count 2, he is claiming injury for “Intrusion Upon Seclusion.” This too is not a claim for “damages for personal injury.”

Fourth, 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 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,<sup>4</sup> alleges that he is an Ethiopian-born citizen of the United States (*see* Complaint 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). Once infected, the program allows an operator in a distant land access to the infected computer thereby enabling the operator to read documents on the computer and to read email that have already been sent or already been received and web searches that have already been conducted.

Plaintiff claims that his computer was infected by “an email” with FinSpy, sent by Defendant or someone operating on its behalf. Complaint at ¶ 5. According to the Complaint, the spyware “then took what amounts to complete control over Plaintiffs computer. Afterwards, it began copying and sending some, if not all, of the activities undertaken by users of the computer, including Plaintiff and members of his family to a server in Ethiopia.” *Id.* 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

---

<sup>4</sup> 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.

Complaint goes on to allege that “Ethiopia had unlimited access to [Plaintiff’s] computer via the transmission of his activities to the Ethiopia server.” *Id.* at ¶ 10 (emphasis added). The spyware “made surreptitious audio recordings of dozens of” Plaintiff’s “Internet phone calls, recorded portions or complete copies of a number of emails sent by [Plaintiff], and recorded a web search.” *Id.* at ¶ 4. 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). Plaintiff presented no evidence that Defendant Ethiopia had anything to do with the alleged viral infection of his computer.

**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. *Verlinden B. V. v. Central Bank of Nigeria*, 461 U. S. 480, 488-489 (1983); *see* 28 U. S. C. § 1604; Joseph Dellapenna, *Suing Foreign Governments and Their Corporations* 11, and n.64 (1988). Under 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 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.

28 U. S. C. § 1605(a)(5).

## **II. The Tort Exception Does Not Apply to the Allegations in the 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) (citing *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d at 1524 (“The legislative history makes clear that for the exception of § 1605(a)(5) to apply ‘the tortious act or omission must occur within the jurisdiction of the United States.’ House Report, *supra*, at 21, 1976 U.S. CODE CONG. & AD. NEWS 6619.”)). See *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.”). This position follows from both the language of the FSIA and from the Supreme Court’s decision in *Amerada Hess Shipping*: “the exception in § 1605(a)(5) covers only torts occurring within the territorial jurisdiction of the United States.” 488 U.S. at 441. The holdings of this and other

circuits that the entire tort must take place in the United States is further buttressed by *Kiobel v. Royal Dutch Petroleum Co.*, \_\_\_ U.S. \_\_\_, 133 S.Ct. 1659, 1664 (2013), where the Court held, in the context of the Alien Tort Statute, that there is a strong presumption against asserting civil jurisdiction for torts over actions that occurred outside the United States. *Kiobel* is particularly relevant given that the legislative history of the Alien Tort Statute suggests, and the tort exception to FSIA expressly indicates, that both were designed to remedy rudimentary torts committed in their entirety in the United States, such as assault on a foreign ambassador in the case of the ATS (*see Kiobel*, 133 S.C. at 1666) and common traffic accidents in the case of the FSIA. *See Amerada Hess Shipping*, 488 U.S. 428, 439-440 (1989) (“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.”).

Here, as alleged in the 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 the computer with the spyware that invaded and controlled his computer was located in Ethiopia. *See* Complaint 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 Complaint goes on to allege that “Ethiopia had unlimited access to Mr. Kidane’s computer via the transmission of his activities to the Ethiopia server.” Complaint at ¶ 10 (emphasis added). 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.” Complaint at ¶ 85 (emphasis added).

Inasmuch as both the *actus rea* and *mens rea* occurred overseas, the two alleged intentional torts have their *situs* overseas. The installation of the software in Plaintiff’s computer



and the control of that software and his computer all occurred allegedly from or in Ethiopia. Since the server and spyware were both located in Ethiopia, we must assume that the human operators also were located in Ethiopia and that any intent necessary to support the two alleged intentional torts was also formulated in Ethiopia. Nothing in the Complaint indicates otherwise. Since the alleged tort and the alleged tortfeasors were allegedly located in and operated in Ethiopia, the entirety of the tort was not alleged have to take place in the United States, but rather in Ethiopia. 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 this 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 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 him was “politically motivated.” *See* Complaint at ¶¶ 22-25; Exhibit B. As such, the alleged activities are, by definition, discretionary functions within the meaning of the FSIA and FTCA.

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 Statutory Damages or to Injuries for Annoyance, as Alleged in this 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"). The statute 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*, p. 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). Plaintiff has not alleged that he has suffered any “mental distress.”

Only once in Plaintiff ‘s lengthy complaint does he allege that he suffered “personal injury,” but the nature of those injuries are never described. Complaint at ¶ 15 (“Defendant or Defendant’s officials or employees caused personal injury to Plaintiff”). Given that “personal injury” is jurisdictional, Plaintiff has to do more than merely make a bald assertion that he suffered personal injury. *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”).

**D. The Tort Exception Does Not Apply to Either Violations of the Wiretap Act or Common Law “Intrusion Upon Seclusion”**

**1. Pleadings Do 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). Here, the anonymous Plaintiff alleges that Defendant violated section 2511 “by [the] unlawful interception of Plaintiffs communications.” Complaint at ¶¶ 15 and 91. No other provisions of the Wiretap Act are referenced in the Complaint. The “interception” provision of section 2511 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)(a). 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.”).<sup>5</sup> Here, the presumption is conclusive. The definition of person includes certain sovereigns, such as the 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), 2511, 2517(6), 2517(8).

---

<sup>5</sup> 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.

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. Complaint Fails to Allege a Necessary “Interception” to Support a Wiretap Act Claim**

The activities hypothesized in the 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.*, Complaint at ¶ 87 (“On information and belief, the FinSpy software used the downloaded modules to intercept Plaintiffs communications 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). *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 extant Complaint.

Here there is no allegation that the defendant acquired any information contemporaneously with its communication. To the contrary, the Complaint is 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 has not pled a violation of the Wiretap Act.

## **2. Common Law Torts, Such as Intrusion Upon Seclusion, Are Expressly Preempted by the Wiretap Act**

With respect to interception, 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.A. § 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).<sup>6</sup> 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 dismissed with prejudice.

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

---

<sup>6</sup> 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); *State v. Williams*, 94 Wash. 2d 531 (1980). 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).



