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

| | |
|---|---|
| John Doe, a.k.a. Kidane,<br><br>Plaintiff,<br><br>v.<br><br>Federal Democratic Republic of Ethiopia,<br><br>Defendant. | Civ. No. 1:14–cv-00372–CKK<br><br>**ORAL ARGUMENT REQUESTED** |

# Plaintiff's Opposition to Defendant's Motion to Dismiss First Amended Complaint

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Cases**

**Statutes**



**Other Authorities**



**U.S. Congress**

## INTRODUCTION

Defendant's Motion to Dismiss the First Amended Complaint should be denied because Defendant has failed to carry its "burden of proving that the plaintiff's allegations do not bring its case within a statutory exception to immunity." *Gulf Res. Am., Inc. v. Republic of Congo*, 370 F.3d 65, 70 (D.C. Cir. 2004) (internal citations and quotation marks omitted).

Plaintiff's First Amended Complaint (the "FAC") establishes that Defendant intercepted Plaintiff's communications in violation of the Wiretap Act, and intruded upon Plaintiff's seclusion. Specifically, the FAC alleges that Defendant, acting through sophisticated spyware software (that is licensed only to governments) installed on Plaintiff's Maryland-based computer, contemporaneously intercepted and recorded Plaintiff's private Skype conversations; and also contemporaneously monitored and recorded Plaintiff's private web browsing and e-mail activity.

Defendant's contention that it is immune from the allegation that it installed spyware and intentionally eavesdropped on a United States citizen, residing in the United States, ignores both the realities of the digital age in which we live and the law under which this motion must be decided.

Defendant's primary argument, that the entirety of the tort occurred outside the United States, is premised upon considering only the acts of Defendant's government agents in Ethiopia, and disregarding the acts of Defendant's software agent (its spyware) in the United States. Although it is true that *some* conduct occurred in Ethiopia, that conduct is peripheral to the conduct underlying the elements of the asserted claims – the operation of the spyware software installed by Ethiopia on a U.S. citizen's U.S computer. The conduct that is relevant to

Plaintiff's claims occurred in the United States through a software program that Defendant licensed, disseminated, and activated, intending it to monitor and intercept Plaintiff's activities.

Defendant's apparent belief that the acts of its software program are distinct from its own acts, is both archaic and untenable.[1] In today's modern age, one can inflict substantial harm in countries thousands of miles away, all without physically crossing a single border or even leaving one's desk. Armed with sophisticated software and enabled by the interconnectedness of the Internet, one can personally access a computer in a foreign land, or one can deploy a computer program to achieve the same result. Despite the distance in space and, potentially, time, these acts remain attributable to the individual.

In order for United States law to protect its citizens, it must be applied such that a person's acts are not rigidly limited to the person's physical location. Indeed it never has been – Ethiopia would be as liable if it accomplished its wiretapping through a human agent as it is for using a digital one. Any distinction between the two approaches is artificial. And although one may be physically present in another country, by virtue of modern technology he or she can be "virtually" present in the United States either through an internet connection acting as a portal, or through software that is, itself physically present in the United States, acting as their agent. In either case, for all intents and purposes it is as though the person is physically present and accessing files on the target computer, just as a flesh and blood individual would access a file cabinet decades ago.

---

[1] The consequences of adopting Defendant's skewed view of the law are unsettling, to say the least. Rogue nations would be empowered to remotely drain U.S. citizens' bank accounts, or to hack and shut down power grids, etc., all on account of the characterization that the entirety of the tort would not have occurred in the United States.

The fact that the governments or persons directing or initiating computer intrusions are physically located outside the United is not a loophole through which they can escape liability. A person's presence and acts are extensible to the location of a computer he or she accesses, or an agent (human or digital) he or she deploys. Here, Defendant deployed a software program that, while physically present on Plaintiff's Maryland computer, monitored and recorded Plaintiff's computer activities. Thus, the entirety of the torts alleged here occurred within the United States.

Ethiopia's additional arguments fare no better than the first. Through a strained reading of the Wiretap Act, Ethiopia argues that it is not an "entity," thereby rendering portions of the statutory language superfluous; and that its eavesdropping on Kidane was not "contemporaneous" because the FinSpy files were not transmitted to Ethiopia at the same time they were being recorded. Ethiopia also seeks to characterize its eavesdropping on a U.S. citizen as a discretionary function that is immune from judicial review, even though it is an illegal act. And throughout, Ethiopia erroneously implies that the Court should draw all factual inferences in Ethiopia's favor, rather than Plaintiff's as the law requires. As demonstrated below, these arguments too are without merit.

Defendant's motion to dismiss should be denied. Given the this case's potential for precedent — where a foreign government installed surveillance software to eavesdrop on U.S. citizens — Plaintiff Kidane respectfully requests, under Local Rule 7(f), that this Court permit an oral hearing on Defendant's motion.

## STATEMENT OF THE CASE

Although Defendant used complex technology, this case is straightforward. Mr. Kidane alleges that Defendant, the Federal Democratic Republic of Ethiopia ("Defendant" or "Ethiopia"), violated the Wiretap Act by intentionally eavesdropping upon telephone calls made through his computer from his home in Maryland.[2] In addition, Ethiopia intentionally monitored Mr. Kidane's Web browsing and e-mail usage on his home computer, thereby committing an intrusion upon his seclusion.[3]

The technology that Ethiopia used to compromise Mr. Kidane's computer, record his phone calls, and monitor his Web browsing, was not a virus or even a technology available to non-governmental parties. Rather, it was FinSpy, a commercial software product designed for — and licensed exclusively to — governments.[4] While the initial infection method resembles a computer virus, the command-and-control infrastructure that controls FinSpy, as well as its software licensing model and expense, have little in common with hackers' tools.[5]

Ethiopia compromised Mr. Kidane's computer after he opened a Microsoft Word document that an acquaintance e-mailed him.[6] Hard-coded in that document was the IP address of the command-and-control server to which Mr. Kidane's computer reported back throughout the infection.[7] That server was located in Ethiopia, on a block of IP addresses owned by the official state-run ISP

---

[2] *See* Plaintiff's First Amended Complaint ("FAC") at ¶¶ 92–100.

[3] *See* First Am. Compl. ¶¶ 101–105.

[4] *Id.* ¶¶ 6, 26–54, Exhibit A.

[5] *Id*.

[6] *Id*. ¶¶ 5, 56, Exhibit C.

[7] *Id*. ¶¶ 43, 58, 77.

of Ethiopia, and controlled by the Defendant.[8] While Mr. Kidane may not have been the original target of Ethiopia's surveillance, Ethiopia nonetheless intentionally activated the infection on Mr. Kidane's computer in Maryland, kept the infection active from October 31, 2012 until March 18, 2013, and disabled it five days after the University of Toronto's Citizen Lab publicly disclosed Defendant's use of FinSpy.[9] FinSpy licenses to governments only allow a certain number of infected devices to be concurrently monitored so Ethiopia's monitoring Mr. Kidane counted toward the total number of monitoring devices Ethiopia could keep active at any one time.[10]

While Mr. Kidane's computer was actively infected, Ethiopia used FinSpy to contemporaneously record dozens (and perhaps hundreds) of Mr. Kidane's Skype Internet phone calls, using the FinSpy software that Ethiopia installed on Mr. Kidane's his computer in Maryland.[11] In addition, Ethiopia monitored and recorded Mr. Kidane's Web browsing history and e-mail usage, as well as that of his family — again using the FinSpy software that Ethiopia installed on Mr. Kidane's Maryland-based home computer.[12]

After Ethiopia was caught red-handed and publicly exposed by the University of Toronto's Citizen Lab for operating a FinSpy relay—the same relay it used here—Ethiopia sought to cover its tracks, attempting to erase from Mr. Kidane's computer the evidence of Ethiopia's spying.[13] But because FinSpy had a

[8] *Id*. ¶¶ 57–62.

[9] *Id*. ¶¶ 75–77.

[10] *Id*. ¶44, Exhibit A.

[11] *Id*. ¶¶ 65–69.

[12] *Id*. ¶¶ 74–77.

[13] *Id*. ¶¶ 50, 61–64, 70–71, Exhibit B.

technical failure, Ethiopia's attempt to wipe all traces of FinSpy from Mr. Kidane's computer failed, allowing him to discover the intrusion and track it to the Ethiopian government.[14] This lawsuit ensued.

## ARGUMENT

### I. Ethiopia bears the burden of proving immunity from suit under the FSIA

When the Ethiopian government acts within the United States, it is subject to United States law. The Foreign Sovereign Immunities Act (FSIA), 28 U.S.C. §§ 1330, 1602–1611, provides the basis for jurisdiction against the government of Ethiopia. *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 439 (1989). This Court has subject matter jurisdiction over "any claim for relief in personam" for which Ethiopia "is not entitled to immunity" under one of the statutory exceptions to immunity in the FSIA. 28 U.S.C. § 1330

While the FSIA does provide limited immunity from some civil claims in the United States, that statute has a "restrictive view of sovereign immunity." Under it, Ethiopia "bears the burden of proving that the plaintiff's allegations do not bring its case within a statutory exception to immunity." *Gulf Res. Am., Inc. v. Republic of Congo*, 370 F.3d 65, 70 (D.C. Cir. 2004) (internal citations and quotation marks omitted). As with any 12(b)(1) motion, the Court must accept as true all uncontroverted material factual allegations contained in the complaint and "construe the complaint liberally, granting plaintiff the benefit of all inferences that can be derived from the facts alleged and upon such facts determine

[14] *Id.*

jurisdictional questions." *Am. Nat'l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011) (citations omitted).

Here, Ethiopia has not met its burden to demonstrate immunity. To the contrary, Plaintiff's allegations are more than sufficient to trigger the FSIA's non-commercial tort exception (the "tort exception"), which denies immunity in cases like this:

> 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).

Plaintiff seeks (1) money damages against Ethiopia[15] for (2) personal injuries to Plaintiff's feelings and intimate privacy rights[16] (3) caused by the tortious invasion of Plaintiff's family computer and interception of Plaintiff's private communications.[17] This electronic home invasion was (4) carried out by Ethiopia via a recording device installed and operated in Plaintiff's home in Silver Spring, Maryland, under the control of Ethiopia's officials or employees.[18] Because

---

[15] *Id.* ¶¶ 12, 100, p.23 at ¶ 2.

[16] *Id.* ¶¶ 13, 15, 69, 77, 87, 91, p.23 at ¶ 2.

[17] *Id.* ¶ 4, 69, 77, 87, 91, 95–99, 102–105.

[18] *Id.* ¶ 5–6, 8, 10–11, 77, 79–91.

Plaintiff's allegations of wiretapping and intrusion upon seclusion under federal and Maryland law sufficiently set forth a claim for money damages against Ethiopia, those same allegations waive Ethiopia's immunity under the FSIA's tort exception.

## II. The FSIA tort exception waives Ethiopia's immunity for Plaintiff's claims of tortious, non-discretionary acts and injuries occurring in the United States.

### A. The tort exception applies to violations of the Wiretap Act and common law intrusion upon seclusion.

#### 1. Ethiopia's recording of Plaintiff's Skype calls unambiguously violated the Wiretap Act.

Ethiopia's first argument is the very troubling claim that a foreign government should be completely immune from liability under the Wiretap Act. While Plaintiff could find no precedent directly on point, many cases lead to the conclusion that Ethiopia does not enjoy any broad right to wiretap Americans. That conclusion is consistent with similar caselaw and, more importantly, comports with common sense. This Court should reject the Ethiopian government's invitation to grant it (and any other foreign government) any *carte blanche* ability to wiretap American citizens on American soil. As described further below, neither the U.S. government nor any state or local government in the U.S. would be immune from suit for such actions. Moreover, to the extent that it requires evidence collected in the United States, Ethiopia has potential recourse were it to enter into an agreement under the Mutual Legal Assistance Treaty

("MLAT").[19] Indeed, Ethiopia's proposed interpretation of the FSIA would render that regime superfluous.

**a. Ethiopia's recordings of Plaintiff's Skype calls were Wiretap Act interceptions.**

The Wiretap Act defines "interception" as "the aural or other acquisition of the contents of any wire, electronic, or oral communications through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Ethiopia did just that, using a product called FinSpy sold by a company called Gamma.[20] As noted above, FinSpy is licensed only to governments. Plaintiff alleges,[21] Gamma's own marketing materials show,[22] expert testimony will demonstrate, and logic dictates that when Ethiopia used FinSpy to record Mr. Kidane's telephone calls, that contemporaneous recording triggered Wiretap Act liability.

The Defendant attempts to sidestep liability first, by claiming that while Ethiopia digitally intercepted Mr. Kidane's Skype calls, those were not "interceptions" under the Wiretap Act. Instead, Ethiopia claims — without support — that to constitute a wiretap violation under the Wiretap Act, there must be *simultaneous transmission to the eavesdropper*. Not so. "The recording of a telephone conversation alone constitutes an 'aural . . . acquisition' of that conversation." *See Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir.1994) (citations omitted; modification in original). Thus, when a manager installed

---

19 U.S. Dep't of State, "Treaties and Agreements" 2012, <http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm>. The fact that Ethiopia does not have an MLAT in place does not give it the power to act with impunity.

20 *E.g.,* First Am. Compl. ¶¶ 26, 37–38, 65, 77.

21 *Id.*

22 *See id. at* Exhibit A.

voice-activated tape recorders on a telephone system, he "intercepted" employee calls even though he listened to the calls later. *Pascale v. Carolina Freight Carriers Corp.*, 898 F. Supp. 276, 279–80 (D.N.J. 1995). Similarly, the Fifth Circuit properly focused on the time when communications are recorded:

> The words "acquisition . . . through the use of any . . . device" suggest that the central concern is with the activity engaged in at the time of the oral communication which causes such communication to be overheard by uninvited listeners. If a person secrets a recorder in a room and thereby records a conversation between two others, an "acquisition" occurs at the time the recording is made.

*United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976) (omissions in original). The Eleventh Circuit has also confirmed that the Wiretap Act can be violated even when the communications are recorded but not actually heard. *United States v. Nelson*, 837 F.2d 1519, 1527 (11th Cir. 1988).

**b. Governmental entities, including foreign sovereigns, are civilly liable under the Wiretap Act.**

Defendant's next argument — that as a foreign sovereign, it falls outside the definition of persons who can violate the Wiretap Act —also fails. Congress amended the Act to include a governmental "entity" like Ethiopia.

Section 2520 of the Wiretap Act provides the basis for this and all other civil Wiretap Act suits. In 1986, Congress amended that section to "add[] the words 'or entity' to those who may be held liable under the Act." *Adams*, 250 F.3d at 985; *see also Williams*, 393 F. Supp. 2d at 1132 ("[P]rior to 1986, the section creating civil liability referred only to a cause of action against a 'person;' that year, the Congress amended the civil liability section to read . . . '*or entity*'") (emphasis in original). Courts interpreting the Act draw a distinction between *criminal* liability under Section 2511 of the Act, which applies only to "persons," and *civil* liability

under Section 2520, which is more expansive and includes governmental entities. *Conner*, 130 F. Supp. 2d at 1373–75.

As a result, most courts have held that (1) Section 2520 creates civil liability under the Wiretap Act; (2) the phrase "or entity" as added to the Act in 1986 logically must refer to governmental entities in order to have meaning and effect; and (3) the legislative history with respect to the similarly amended Stored Communications Act suggests that Congress intended "entity" to mean governmental entity.[23] As the Sixth Circuit noted: "the 1986 amendments [to 18 U.S.C. § 2520] indicate that a governmental entity may be liable in a civil suit under the Act." *Adams v. City of Battle Creek*, 250 F.3d 980, 985 (6th Cir. 2001); *see Organizacion JD Ltda. v. U.S. Dep't of Justice*, 18 F.3d 91, 94–95 (2d Cir. 1994); *Williams v. City of Tulsa. OK*, 393 F. Supp. 2d 1124, 1132 (N.D. Okla. 2005); *Conner v. Tate*, 130 F. Supp. 2d 1370, 1373–75 (N.D. Ga. 2001); *Dorris v. Absher*, 959 F. Supp. 813, 820 (M.D. Tenn. 1997) *aff'd in part, rev'd in part*, 179 F.3d 420 (6th Cir. 1999); *PBA Local No. 38 v. Woodbridge Police Dep't*, 832 F. Supp. 808, 823 (D.N.J. 1993); *Garza v. Bexar Metro. Water Dist.*, 639 F. Supp. 2d 770, 774–775 (W.D. Tex. 2009).

### c. The phrase "or entity" added in 1986 would be superfluous if it didn't refer to governmental entities.

Specifically, courts have correctly observed that failing to find that "entity" refers to governmental entities would render the 1986 amendment superfluous. The Second Circuit has held that: "in order to give full meaning to the new

---

23 Defendant's argument — that if it is amenable to suit under the Wiretap Act, then it must therefore be a person for the purpose of the Fifth Amendment — is without import. As discussed in Section I, the Foreign Sovereign Immunities Act creates this Court's jurisdiction over the Ethiopia, regardless of any minimum-contacts analysis. But in any case, Ethiopia's conduct of spying in Maryland is more than enough to support personal jurisdiction.

statutory language [of Section 2520], 'entity' must be taken to mean governmental entity." *Organizacion JD Ltda.*, 18 F.3d at 94–95. This is because "the definition of 'person' already included business entities such as corporations and partnerships," so "entity" could only refer to governmental entities. *Id.; see also Adams*, 250 F.3d at 985 ("In order for the term not to be superfluous, the term 'entity' necessarily means governmental entities.").

The court in *Williams* further reasoned that "Congress' subsequent amendment in 2001 to exclude the United States from entities that could be liable evidences a Congressional understanding that the 1986 amendment created governmental liability." *Williams*, 393 F. Supp. 2d at 1132–33; *see also Garza v. Bexar Metro. Water Dist.*, 639 F. Supp. 2d at 774 ("There would have been no reason for Congress to carve out an exception for the United States if governmental entities could not be sued under the statute."). The government of Ethiopia is undoubtedly a governmental entity.

**d. Congress expressly intended similar language added to the Stored Communications Act to apply to governmental entities.**

Additional support for this conclusion is found in the legislative history, which can be consulted if the statutory language is deemed to be ambiguous. *See Conner*, 130 F. Supp. 2d at 1374 (citing *United States v. McLemore*, 28 F.3d 1160, 1162 (11th Cir. 1994)). Because the legislative history of the 1986 amendment to the Wiretap Act is silent as to the meaning or effect of "entity" in the amendment, some courts have looked to the addition of the same language to the civil liability for interception of stored wire and electronic communications under 18 U.S.C. § 2707(a). *Adams*, 250 F.3d at 985; *see also Williams*, 393 F. Supp. 2d at 1132 ("What limited legislative history exists is silent on the addition of this language . . .")

(citing 147 Cong. Rec. H. 7159, 7198 (Oct. 23, 2001); 147 Cong. Rec. S. 10990, 11007 (Oct. 25, 2001)).

The Stored Communications Act's section 2707(a), as amended, includes the same "or entity" phrasing as the Wiretap Act's section 2520. The Senate report summarizing that section makes clear that Congress's intention was that a civil cause of action for damages be created against "any person or entity—*including governmental entities*—who knowingly or intentionally violated this chapter." S. Rep. No. 541, 99th Cong., 2d Sess. 43 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3597 (emphasis added); *see Bodunde v. Parizek*, 93 C 1464, 1993 WL 189941 at *3–4 (N.D. Ill. May 28, 1993).

This Court should follow those courts that have held that the legislative history supports constructing the statute to impose civil liability on governmental entities. *See Dorris*, 959 F. Supp. at 820 ("Based on the language of the statute and its amendments, the legislative history, and the weight of the case law that has considered the issue, the Court holds that governmental entities may be held liable under Section 2520."); *Conner*, 130 F. Supp. 2d at 1374 (following other courts' holdings that the Senate Committee Report on § 2707 constitutes "sufficient legislative history to conclude that governmental entities may be liable under the Wiretap Act").

### 2. Ethiopia's monitoring of Plaintiff's Web usage was an unambiguous intrusion upon his seclusion.

Defendant appears to argue that it cannot be liable for intruding Mr. Kidane's seclusion because it initially intended to intrude upon someone else's seclusion — and only accidentally started spying on Mr. Kidane in October,

2012.[24] Ethiopia's misplaced spying target claim may be true, and the Complaint takes this possibility into account,[25] but it is irrelevant. Ethiopia intended to spy, and that is sufficient for the tort of intrusion upon seclusion. Moreover, once the Ethiopian FinSpy spyware infected Mr. Kidane, Ethiopia continued to spy on him — and pay for it under the FinSpy billing practices — for several months.[26] The spying stopped only when Ethiopia's spying was discovered.[27]

As with all intentional torts, the intent element for the tort of intrusion upon seclusion is whether the act was one of volition. Here, the intent that matters is that Defendant intended to spy on someone, and the Complaint sufficiently alleges that point.[28] Just as someone would still be liable for accidentally peeping into the wrong bedroom window, Ethiopia cannot escape liability by claiming that it lacks sufficient intent, because — while it intended to spy — it only accidentally spied on Mr. Kidane, at least initially.

Equally important, however, whatever intent Ethiopia may have lacked initially was gained when it *kept* spying on Mr. Kidane for another five months after the spyware's installation, until it was caught in March 2013. As noted above, FinSpy charges per installation, so Ethiopia apparently paid to spy on Mr. Kidane. Thus regardless of whether the initial installation was accidental, Plaintiff has sufficiently alleged the requisite intent.

---

[24] *See* Mot. to Dismiss, pp. 19–20.

[25] *See* First. Am. Compl. ¶¶ 5, 56, 81–83.

[26] *See id.* ¶¶ 44, 45, 77.

[27] *See id.* ¶¶ 8–10, 62–63, 77, 88.

[28] *See id.* ¶¶ 5, 56, 81–83.

### B. The tort exception applies because Ethiopia wiretapped a U.S. citizen in the privacy of his home on U.S. soil.

In next arguing that the torts occurred abroad, Ethiopia misses a simple fact: every element of the asserted claims occurred in the United States — from the installation of spyware on a U.S. computer, to the interception of electronic communications in the United States. This case challenges Ethiopia's wiretapping of a U.S. citizen on U.S. soil. It would baffle any U.S. citizen to learn that the surreptitious recording of his words, in the privacy of his American home, is somehow a completely overseas occurrence — as Ethiopia insists.

Fortunately, that is not the law of this or any Circuit. The FSIA tort exception applies whenever the tort's "essential locus"—i.e., the injury and the act that proximately causes that injury—occurs in the United States. *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1524–25 (D.C. Cir. 1984); *accord Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 441 (1989) (noting that the tort exception does not apply to foreign conduct merely because it results in domestic injury).

Here, the United States is the "essential locus" of the torts of wiretapping and invasion of privacy, because that is where Plaintiff's computer was when it was accessed and infected with spyware, and where he was when his communications were intercepted by Ethiopia's FinSpy device.[29] 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

[29] First Am. Compl. ¶ 77 ("FinSpy operated on Plaintiff's computer in Maryland.").

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)

Here, during the interception, both the people being recorded (Mr. Kidane and his family) and the recording device that captured them were located in Maryland. The contents of Plaintiff's communications were captured by the FinSpy device installed on the computer at Plaintiff's home in Silver Spring, Maryland. The Complaint so alleges: "the recordings of Plaintiff's communications were made automatically, and entirely on Plaintiff's computer in the United States, without intervention of the Ethiopian Master Server."[30] Specifically, FinSpy intercepted Plaintiff's Skype calls by recording audio from the microphone of Plaintiff's computer, capturing the sound of Plaintiff's voice in real-time as he spoke in the privacy of his home.[31] 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).

Similarly, the *situs* of Plaintiff's intrusion-upon-seclusion claim is his home in the United States. Under Maryland law, "[t]he gravamen of th[is] tort is the intrusion into a private place or the invasion of a private seclusion that the plaintiff has thrown about his person or affairs." *New Summit Assocs. Ltd. P'ship v. Nistle*, 533 A.2d 1350, 1354 (Md. App. 1987). Here, the gravamen of the tort

[30] First Am. Compl. ¶ 65.

[31] *Id.* ¶¶ 66–68.

occurred in the United States, because the "intrusion into a private place" happened in Maryland. That is where the FinSpy device "downloaded modules . . . onto Plaintiff's computer,"[32] and used them to "access Plaintiff's most sensitive private communications, including those involving []his work with the Ethiopian Diaspora."[33] And it is where Ethiopia—acting through FinSpy—accessed, recorded, and stored "private details of his family's computer usage" on the hard disk of Plaintiff's computer in Maryland, without Plaintiff's consent.[34] It was this unauthorized access and recording that proximately caused injury to Plaintiff's feelings and the integrity of his privacy—and it occurred wholly in the United States.

This *situs* principle is the norm for computer torts and crimes. Remote computer intrusions occur at the location of the trespassed device: "The fact that the computers were accessed by means of a complex process initiated and controlled from a remote location does not alter the fact that the accessing of the computers . . . [that was] prohibited by the statute, occurred at the place where the computers were physically located." *United States v. Ivanov*, 175 F. Supp. 2d 367, 371 (D. Conn. 2001) (holding that a Russian hacker's intrusion upon computers in Connecticut violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4), in the United States); *see also Am. Online, Inc. v. Nat'l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1270 (N.D. Iowa 2000) (finding, for choice of law purposes, that Virginia was the *situs* of an Iowa corporation's unauthorized electronic access of AOL hardware located in Virginia).

---

[32] First Am. Compl. ¶ 86.

[33] *Id.* ¶ 91.

[34] *Id.* ¶ 77.

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. Because interception occurs even without listening, *In re State Police Litig.*, 888 F. Supp. 1235, 1267 (D. Conn. 1995), 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.[35]

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.*; *see also Liu v. Republic of China*, 892 F.2d 1419, 1434 (9th Cir. 1989) (applying tort exception to the alleged assassination of a U.S. resident in California

35 The Complaint's allegations that the FinSpy Relay was located in Ethiopia, First Am. Compl. ¶¶ 58–62, with an IP address registered to Ethiopia's state-owned telecommunications company, *id.* ¶ 59, serve to identify Ethiopia as the responsible entity; they do not change the fact that the interception happened in the United States.

by agents acting under the remote supervision of the Republic of China). Similarly, the U.S. District Court for the District of Columbia held that neither the FSIA nor the act-of-state doctrine would protect a foreign government from civil liability if it ordered and remotely directed an assassination that took place in Washington, D.C. *Letelier v. Republic of Chile*, 488 F. Supp. 665, 673–74 (D.D.C. 1980). The D.C. and other circuits continue to cite *Letelier* with approval. *See, e.g.*, *MacArthur Area Citizens Ass'n v. Republic of Peru*, 809 F.2d 918, 922 n.4 (D.C. Cir. 1987); *Doe v. Bin Laden*, 663 F.3d 64, 69 (2d Cir. 2011); *Liu*, 892 F.2d at 1432.

Nevertheless, Ethiopia maintains that it has immunized itself from liability by remotely intruding into Plaintiff's home and private affairs in Maryland. In effect, Ethiopia's conduct is no different than if it had sent a flesh-and-blood agent into Plaintiff's house to install a recording device. In the past, Ethiopia would have had no alternative. The fact that Ethiopia has now acquired the technological means to spy on U.S. citizens on U.S. soil without sending a human agent does not mean it can suddenly circumvent U.S. wiretapping laws or claim sovereign immunity for the torts it commits remotely: remote intrusions have the same legal consequences as physical intrusions. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion . . . constitutes a search.") (internal quotation marks omitted).[36]

In fact, the Ninth Circuit has cautioned against precisely the sort of logic-defying, artful pleading that Ethiopia displays here: "requiring every aspect of the tortious conduct to occur in the United States . . . would encourage foreign states

36 Indeed, Congress enacted the Electronic Communications Privacy Act to keep pace with remote surveillance technology: "Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances." S. Rep. No. 99-541, at 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555.

to allege that some tortious conduct occurred outside the United States." *Olsen*, 729 F.2d at 646. 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).

All the same, Ethiopia tries to paper over the fact that it wiretapped a U.S. citizen on U.S. soil with reams of inapposite case law. None of these cases share a nexus with the United States comparable to Ethiopia's wiretapping of Plaintiff in his Maryland home. For example, Ethiopia relies on a case where a tanker was bombed on the high seas. *Amerada Hess*, 488 U.S. at 439–40. Obviously, in that case, neither the tortious act nor the injury occurred in the United States.

Similarly, Ethiopia tries to convert *SEDCO*, a 32-year-old Southern District of Texas decision, into the law of the D.C. Circuit. Def's Mem. at 7, citing *In re SEDCO, Inc.*, 543 F. Supp. 561, 567 (S.D. Tex. 1982). But in *SEDCO*, *none* of the alleged acts or omissions from a Mexican oil rig explosion occurred in the United States — only the resultant injuries. *See SEDCO*, 543 F. Supp. at 567. *SEDCO* might guide the present matter if the oil rig—like Ethiopia's FinSpy device—had been operated in U.S. territory. But it was not, so *SEDCO*'s "entire tort" rule refers to a very different factual scenario.

In fact, each of Ethiopia's cited cases is distinguishable on the same ground: unlike here, none involved a tortious act completed in the United States. *See Van Dardel v. Union of Soviet Socialist Republics*, 736 F. Supp. 1, 7 (D.D.C. 1990) (detention and death of victim **in Hungary** is not actionable under tort exception); *Persinger v. Islamic Republic of Iran*, 729 F.2d 835, 842 (D.C. Cir. 1984) (detention of American hostages at U.S. embassy **in Tehran** not actionable); *Jerez v. Republic of Cuba*, 777 F. Supp. 2d 6, 25 (D.D.C. 2011) (abuse during psychiatric confinement

**in Cuba** not actionable); *Coleman v. Alcolac, Inc.*, 888 F. Supp. 1388, 1403 (S.D. Tex. 1995) (exposure of U.S. soldiers to chemical weapons **in Iraq** not actionable); *Four Corners Helicopters, Inc. v. Turbomeca S.A.*, 677 F. Supp. 1096, 1102 (D. Col. 1988) (negligent manufacture of helicopter **in France** not actionable); *Antares Aircraft L.P. v. Fed. Republic of Nigeria*, No. 89 CIV. 6513(JSM), 1991 WL 29287 (S.D.N.Y. Mar. 1, 1991) (conversion of aircraft **in Nigeria** not actionable).[37]

Not one of these cases involved a tortious act completed in the United States such as Ethiopia's interception and intrusions here, which took place entirely in Mr. Kidane's home in Maryland. None serves to bar Plaintiff's claims. Because the tortious interception and intrusion occurred entirely at Plaintiff's home in the United States, the FSIA tort exception waives Ethiopia's immunity.

### C. The tort exception applies because Ethiopia has no discretion to commit criminal wiretapping or to circumvent U.S. regulations on foreign law enforcement cooperation.

Apparently, Ethiopia believes it has unregulated discretion to surveil U.S. citizens in their homes—a discretion that even the U.S. Government does not enjoy. Ethiopia claims that its acts of warrantless wiretapping and computer intrusion were discretionary acts that fall outside the reach of the tort exception.[38] Under § 1605(a)(5)(A), the tort exception does not waive immunity as to "any claim based upon the exercise or performance [of] . . . a discretionary function regardless of whether the discretion be abused." The FSIA's discretionary function

37 Ethiopia's reliance on *O'Bryan v. Holy See*, 556 F.3d 361 (6th Cir. 2009), is also misplaced. In *O'Bryan*, the Sixth Circuit only barred plaintiffs' claims for negligent supervision in Vatican City. *Id*. at 386. Claims involving tortious conduct in the United States were allowed to proceed under the tort exception. *Id*. Plaintiff brings no claims alleging negligent training or supervision in Ethiopia.

38 Def's Mem. at 11–13.

clause was modeled on a clause of the Federal Tort Claims Act, 28 U.S.C. § 2680(a) ("FTCA"), and courts interpret the FSIA in light of FTCA jurisprudence. *See MacArthur Area Citizens Ass'n v. Republic of Peru*, 809 F.2d 918, 921–22 (D.C. Cir. 1987), *modified on other grounds*, 823 F.2d 606 (D.C. Cir. 1987).

The Supreme Court has set forth a two-part test to determine whether an action is discretionary. First, the challenged conduct must involve "an element of judgment of choice." *United States v. Gaubert*, 499 U.S. 315, 322 (1991) (quotations omitted). If the challenged conduct did leave "room for choice," then the court proceeds to *Gaubert* step-two, determining "whether that judgment is of the kind that the discretionary function was designed to shield." *Id.* at 322–23. Specifically, the activity must be "grounded in social, economic and political policy." *Id.* at 323.

Ethiopia fails at step one: an act is not discretionary if it violates a mandatory requirement or prohibition. *Id.* at 324. As the Supreme Court observed in *Gaubert*: "[I]f the employee violates [a] mandatory regulation, there will be no shelter from liability because there is no room for choice and the action will be contrary to policy." If "a federal statute, regulation or policy specifically prescribes a course of action," then there is "no rightful option but to adhere to the directive." *Id.* at 322 (quotation omitted). Ethiopia simply had no discretion to violate the mandatory prohibitions on wiretapping an American citizen at his residence inside the United States provided by U.S. law.

### 1. Ethiopia's agents had no discretion to commit criminal wiretapping in violation of federal law.

Most simply, Ethiopia's actions were not discretionary because they contravened United States criminal laws. *See Gaubert*, 499 U.S. at 322. For decades, courts construing the FSIA tort exception have held that a foreign state has "no

discretion to commit, or to have one's officers commit, an illegal act." *Letelier v. Republic of Chile*, 488 F. Supp. 665, 673 (D.D.C. 1980). As the D.C. Circuit observed, "case law buttresses the proposition that a criminal act cannot be discretionary." *MacArthur Area Citizens Ass'n*, 809 F.2d at 922 n.4; *accord Liu v. Republic of China*, 892 F.2d 1419, 1431 (9th Cir. 1989) (holding that agents of China had no discretion to assassinate a U.S. resident).

Granted, to be non-discretionary, the illegal acts must be sufficiently grave. *See, e.g.*, *MacArthur Area Citizens Ass'n*, 809 F.2d at 924 (holding that a mere zoning infraction in the construction of a chancery does not warrant waiving discretionary-act immunity). And the illegal act must be directly linked to the foreign state and its agents: merely recommending grants to a recipient who later diverts them to a crime is too attenuated a link. *See In re Terrorist Attacks on September 11, 2001*, 349 F. Supp. 2d 765, 802 (S.D.N.Y. 2005) *on reconsideration in part*, 392 F. Supp. 2d 539 (S.D.N.Y. 2005); *Burnett v. Al Baraka Invest. & Dev. Corp.*, 292 F. Supp. 2d 9, 20 (D.D.C. 2003). Also too attenuated is a consular officer giving travel documents to a foreign citizen who later uses them to violate a child custody order. *See Risk v. Halvorsen*, 936 F.2d 393, 397 (9th Cir. 1991). So too is negligently hiring or training an employee who later commits an intentional tort. *See Jin v. Ministry of State Sec.*, 475 F. Supp. 2d 54, 67 (D.D.C. 2007). And while a negligent hiring policy may be a discretionary function, an employee committing a criminal sexual assault is not; the responsible foreign sovereign may be subject to *respondeat superior* liability under the tort exception. *Doe v. Holy See*, 557 F.3d 1066, 1083–85 (9th Cir. 2009). Read together, these cases suggest that a serious felony like wiretapping — committed directly by a state — is non-discretionary.

Here, Ethiopia's illegal wiretapping and computer intrusion were not like zoning infractions, grant recommendations, or consular assistance. First, these

were computer crimes committed directly by state agents and are serious felonies under federal law. *See* 18 U.S.C. § 2511(a) (defining crime of wiretapping). Second, for half a century, federal courts have held that unlawful surveillance and trespassory searches are precisely the sort of criminal acts that are non-discretionary. *See, e.g.*, *Hatahley v. United States*, 351 U.S. 173, 181 (1956) (holding that acts of unlawful trespass, committed by federal agents in violation of a federal range law, were non-discretionary under FTCA); *Birnbaum v. United States*, 588 F.2d 319, 329–30, 332 (2d Cir. 1978) (holding that federal agents who covertly opened the mail of U.S. citizens had no discretion to exercise under the FTCA); *Orlikow v. United States*, 682 F. Supp. 77, 81–82 (D.D.C. 1988) (holding that "[w]hen a decision is made to conduct intelligence operations by methods which are unconstitutional or egregious, it is lacking in statutory or regulatory authority," and outside the discretionary-act exception to the FTCA); *Cruikshank v. United States*, 431 F. Supp. 1355, 1359 (D. Haw. 1977) (holding that warrantless surveillance of mail by federal agents was non-discretionary under FTCA: no "government should . . . have the 'discretion' to commit illegal acts whenever it pleases. In this area, there should be no policy option.").

Since U.S. agents have no discretion to intercept mail or other private communications without judicial or other proper authorization, then *a fortiori*, Ethiopian agents cannot have such discretion. Ethiopia's illegal wiretapping and computer intrusions are not entitled to discretionary function immunity.

### 2. Ethiopia had no discretion to circumvent U.S. regulations on foreign law enforcement cooperation by the warrantless wiretapping of a U.S. citizen on U.S. soil.

Because Ethiopia failed to secure the U.S. government's authorization to engage in wiretapping of Americans inside the U.S., Ethiopia also had no room for

policy judgment. Ethiopia has made no showing that it worked with any U.S. officials, in the United States Department of State or otherwise, to obtain any legal process to lawfully wiretap Plaintiff at his home in Maryland or, more likely, to request that the U.S. conduct the wiretapping on its behalf.

As this Court is aware, electronic surveillance in the United States is a highly regulated activity. 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 for law enforcement, national security, and constitutional rights and civil liberties. 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 to conduct surveillance against 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 Ethiopia and the United States have yet not entered into a mutual legal assistance treaty, this fact gives Ethiopia less—and certainly not more—discretion to conduct wiretapping of Americans in the United States.[39]

Moreover, any foreign law enforcement cooperation in U.S. territory would be subject to American guarantees of individual rights. *See id.* at 572 ("We

[39] *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>.

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 Ethiopia 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 Ethiopia such discretion would perversely incentivize foreign states *not* to cooperate with U.S. law enforcement agencies — and thereby circumvent American privacy regulations and rule of law.

Because Ethiopia 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 Plaintiff's privacy.

### D. Mr. Kidane's tort claims are based on Defendant's affirmative misconduct, not misrepresentation or deceit.

Under 28 U.S.C. § 1605(a)(5)(B), a right of action against a foreign state may proceed for any "tortious act or omission of that foreign state or of any official or employee of that foreign state," so long as the tort claims are not based on, *inter alia*, "misrepresentation" or "deceit." Here, Mr. Kidane's tort claim is based on the Ethiopian government's installation of a malware program on an American citizen's computer, on American soil, and Ethiopia's subsequent interceptions and contemporaneous recordings of dozens of Mr. Kidane's private communications

and Web searches, which were transmitted back to the Ethiopian government to further its well-documented repressive spying efforts.

The Ethiopian government charitably recasts its wiretapping as a mere misrepresentation or deceit, arguing that Mr. Kidane's claim is therefore based on "misrepresentation" or "deceit." But aside from cherry picking two words from the Complaint and misrepresenting them out of context, Defendant's factual and legal support for its argument is strikingly absent. In fact, while Defendant cites the *Tifa* case, the only quotation merely parrots the statutory language. *Tifa, Ltd. v. Republic of Ghana*, No. 88–CV-1513, 1991 U.S Dist. LEXIS 11855, *19, 21 (D.D.C. Aug. 27, 1991). There, unlike here, the plaintiff claimed literal "misrepresentations" made while negotiating a contract to be performed in Ghana. *Id.* at *3–14.

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 intercepting, recording, and transmitting from Maryland — back to Ethiopia — Mr. Kidane's private communications.

Similarly, another court denied a motion to dismiss a claim for conversion under 1605(a)(5)(B), holding that "the claims of misrepresentation and conversion

are distinct causes of action, consisting of different factual elements." *De Sanchez v. Banco Central de Nicaragua*, 515 F. Supp. 900, 912 (E.D. La. 1981).[40]

Courts interpreting section 1605(a)(5)(B) 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, the Court of Appeals for the D.C. Circuit 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 that 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.*

Consistent with the D.C. Circuit'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 — Defendant's motion to dismiss must be denied.

---

[40] While the claims in *De Sanchez* were ultimately dismissed on summary judgment as "in essence a property rather than a tort claim," and thus § 1605(a)(5) was inapplicable, this issue is not relevant here because Ethiopia does not contend that its actions sound in property rather than tort. *See De Sanchez v. Banco Central de Nicaragua*, 770 F.2d 1385, 1398-1399 (5th Cir. 1985). As such, the district court's analysis supporting its denial of the motion to dismiss remains applicable.

### E. Mr. Kidane's claim for intrusion upon seclusion is not preempted by the Wiretap Act.

As an initial matter, defendant'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, the government'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 because Ethiopia is not a "person" within the meaning of the statute. Motion to Dismiss at 16. 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 the *Bunnell* case that Ethiopia now cites, noting that federal laws establish minimum standards — without preempting the state law at issue:

> the analysis in these cases ignores the great weight of authority holding that one of the principal purposes of the federal statute was to establish minimum standards with which states must comply. In that regard, *Bunnell* and *In re Google Inc. Street View* reflect a marked departure from the preemption analysis of courts in this and other districts and circuits in the more than four decades since the Federal Wiretap Act was enacted. In light of the clarity of the 1968 and 1986 Senate Reports that the federal law is intended to establish minimum standards and not to preempt state laws that meet these standards; the long-standing view of the States and courts that States are free to enact legislation that is more restrictive than the federal law; and the rarity with which preemption applies, the Court concludes that the Federal Wiretap Act does not completely preempt California's Invasion of Privacy Act.

*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.").

Similarly, the court in *Sheppard v. Google, Inc.* held that "[t]he only cases discussing the relationship between complete preemption and the ECPA have failed to find complete preemption." 2012 U.S. Dist. LEXIS 173184, at *12 (W.D. Ark. Dec. 6, 2012) (citing *Lane v. CBS Broad., Inc.*, 612 F. Supp. 2d 623, 636 (E.D. Penn. 2009); *In re NSA Records Litig.*, 483 F. Supp. 2d at 939; *Shively v. Carrier IQ, Inc.*, No. C-12–0290 EMC, 2012 U.S. Dist. LEXIS 103237, 2012 WL 3026553, at *2–10

(N.D. Cal. July 24, 2012); *Leong*, 2012 U.S. Dist. LEXIS 59480 (C.D. Cal. Apr. 27, 2012)).

The *Sheppard* court went on to note that the federal law did not completely preempt state law that is "at least as restrictive" as federal law:

> [t]hese cases find complete preemption lacking in ECPA cases for two main reasons. The first is that the much-touted exclusive-remedy provisions were intended, not to take jurisdiction over civil communications cases away from the states, but rather to make clear that in criminal cases—recall that the ECPA is a criminal statute—evidence suppression is not a remedy for an ECPA violation without an underlying Fourth Amendment violation. In short, unless there is a constitutional violation behind a violation of the ECPA, suppression is not a valid remedy. That narrow meaning does not indicate sufficient congressional intent for complete preemption, especially in civil communications cases such as this one. The other reason is that the broader chapter of the ECPA containing the exclusive-remedy provisions, chapter 119, plainly welcomes state regulation in the same field, so long as the state regulation is "at least as restrictive" as the federal regulation.

*Sheppard,* 2012 U.S. Dist. LEXIS 173184 at *14 (internal citations omitted).

In light of the above case law, which Ethiopia faintly acknowledges in its footnote six, Ethiopia's argument that "[i]n the present case, the [Wiretap Act] precludes a court from providing any remedy beyond that which is provided by the Wiretap Act [and therefore] plaintiff lacks Article III standing to pursue any claim other than a claim under the Wiretap Act" fails logically. To the contrary, if states were free to provide remedies beyond those provided for by the Wiretap Act — and this statement is based on courts holding that the Wiretap Act does not completely preempt state legislation in this area — then all other remedies are clearly *not* precluded: defendant's preemption argument fails, and Article III standing exists.

### F. Injunctive relief is available under the FSIA

Under the tort exception to the FSIA, foreign sovereigns are not immune from liability in actions "in which money damages are sought against a foreign state for personal injury . . . occurring in the United States and caused by the tortuous act or omission of that foreign state." 28 U.S.C. § 1605(a)(5) (2008). The face of the statute does not bar plaintiffs from seeking injunctive relief in lawsuits that also seek money damages for personal injury. Additionally, a foreign state is "liable in the same manner and to the same extent as a private individual under like circumstances." 28 U.S.C. § 1606 (2008).

Courts in this district have ordered injunctions against a foreign state (under other FSIA exceptions) where they would have been ordered against a private defendant. *See Bell Helicopter Textron Inc. v. Islamic Republic of Iran*, 764 F. Supp. 2d 122, 128–29 (D.D.C. 2011), *vacated on other grounds*, 892 F. Supp. 2d 219 (D.D.C. 2012) (enjoining Iran's manufacturing of helicopters that diluted and tarnished Bell Helicopter's mark, under the FSIA commercial activity exception); *see also Agudas Chasidei Chabad of U.S. v. Russian Fed'n*, 729 F. Supp. 2d 141, 143, 148 (D.D.C. 2010) (ordering declaratory and injunctive relief for injuries falling under the FSIA expropriations exception). In *Bell Helicopter*, the court based its reasoning on FSIA Section 1606, which subjects foreign states to the same type and degree of liability as private defendants. *Bell Helicopter*, 764 F. Supp.2d at 129. The court found that an injunction was necessary to prevent future injury because plaintiffs demonstrated that Iran would "continue to engage in activities infringing on the plaintiffs' trade dress." *Id.*

### G. Intrusion upon seclusion constitutes a personal injury

Invasion of privacy, of which intrusion upon seclusion is a type, constitutes its own injury separate from intentional infliction of emotional distress. *See Snyder v. Phelps*, 533 F. Supp. 2d 567, 581, 593 (D. Md. 2008) (awarding separate damages for intentional infliction of emotional distress and intrusion upon seclusion, noting that although they are "based on the same incidents," they remain "two separate torts"), *rev'd on other grounds*, 580 F.3d 206 (4th Cir. 2009), *aff'd on other grounds*, 131 S. Ct. 1207 (U.S. 2011). When a person's privacy is invaded, the injury to be redressed is "to the feelings and sensibilities of the person." *Dresbach v. Doubleday & Co., Inc.*, 518 F. Supp. 1285, 1287 (D.D.C. 1981).

Under Maryland law, injuries to the person include injuries to "both body and psyche." *Niedermayer v. Adelman*, 90 B.R. 146, 149 (D. Md. 1988). In *Niedermayer*, the court held that damages sought in a civil action for invasion of privacy, intentional infliction of emotional distress, etc., were exempt from bankruptcy filings under a Maryland law exempting money payable for the "injury of any person." *Id.* at 146-47. The court held that "[u]nless the statute were to limit the claim to bodily injury, it is difficult to assume that the person does not include both body and psyche." *Id.* at 149. It concluded that "[m]ental anguish, damage to reputation, and damages caused by false imprisonment and malicious prosecution [were] therefore equally injury to the person." *Id.* Although invasion of privacy was not explicitly included in this list, it was included in the list of claims the damages that the court ruled were exempt from bankruptcy filings under the personal injury exemption. *See id.* at 146-49.

District of Columbia law is similarly clear, and courts here explicitly treat invasion of privacy as an "injury to feelings," constituting a "personal injury." *Pearce v. E.F. Hutton Grp., Inc.*, 664 F. Supp. 1490, 1499 (D.D.C. 1987); *see also*

*Bernstein v. Nat'l Broad. Co.*, 129 F. Supp. 817, 825 (D.D.C. 1955) (noting that invasion of privacy is a personal injury that includes "outrage to plaintiff's feelings"), *aff'd*, 232 F.2d 369 (D.C. Cir. 1956). In *Bernstein*, the district court noted that "[a]n injury . . . which affects the sensibilities is equally an injury to the person as an injury to the body." *Bernstein*, 129 F. Supp. at 825 (quotation omitted). Therefore, the court reasoned that "a cause of action for the violation of the right of privacy, causing mental suffering to the plaintiff, is an injury to the person." *Id.* (quotation omitted).

*Pearce*, a later case in the District of D.C., relied on *Bernstein* in explaining the difference between the torts of defamation and invasion of privacy. *See Pearce*, 664 F. Supp. at 1499. The *Pearce* court held that, while defamation was an injury to one's reputation, "[i]nvasion of privacy is a personal injury—an injury to feelings." *Pearce*, 664 F. Supp. at 1499 (citing *Bernstein*, 129 F. Supp. at 825).

## CONCLUSION

The operative facts are simple: Defendant, the government of Ethiopia, intentionally and unlawfully eavesdropped on the telephone calls of a U.S. citizen on U.S. soil — and Ethiopia also intentionally and unlawfully monitored that U.S. citizen's Web browsing and e-mail. Mr. Kidane's complaint sufficient alleges the related facts, and his claims all have sound legal bases. No foreign government, including Ethiopia, should be given *carte blanche* permission to wiretap and eavesdrop upon U.S. citizens. For all the reasons discussed above, Ethiopia's motion to dismiss should be denied.

August 18, 2014

Respectfully submitted,

/s/ Nathan Cardozo
Nathan Cardozo (DC SBN 1018696)
Cindy Cohn (admitted *pro hac vice*)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel. (415) 436–9333
Fax (415) 436–9993
nate@eff.org

Richard M. Martinez (admitted *pro hac vice*)
Samuel L. Walling (admitted *pro hac vice*)
John K. Harting (admitted *pro hac vice*)
ROBINS, KAPLAN, MILLER & CIRESI L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402–2015
Tel.: (612) 349–8500
Fax: (612) 339–4181
rmmartinez@rkmc.com

*Counsel for Plaintiff*

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

| | |
|---|---|
| John Doe, a.k.a. Kidane,<br>Plaintiff,<br>v.<br>Federal Democratic Republic of Ethiopia,<br>Defendant. | Civ. No. 1:14–cv-00372–CKK |

**[PROPOSED] ORDER**

UPON CONSIDERATION of Defendant Federal Democratic Republic of Ethiopia's Motion to Dismiss Plaintiff's First Amended Complaint Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) (the "Motion to Dismiss"), and Plaintiff's opposition to said Motion to Dismiss, it is this _____ day of _____, _____ herby,

ORDERED that Defendant's Motion to Dismiss is **DENIED**.

_____
Hon. Colleen Kollar-Kotelly
Judge, U.S. District Court for the
District of Columbia