UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JOHN DOE, a.k.a. KIDANE,

Plaintiff,

v.

FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA,

Defendant.

Civil Action No. 14-372 (RDM)

MEMORANDUM OPINION AND ORDER

The central question presented in this case is whether federal law permits the plaintiff, a U.S. citizen born in Ethiopia who remains active in the Ethiopian diaspora, to maintain suit in this Court against the Federal Democratic Republic of Ethiopia for its alleged surreptitious monitoring and recording of his (and his family's) computer activities and communications in Silver Spring, Maryland. Plaintiff claims that, in doing so, Ethiopia violated Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act"), 18 U.S.C. § 2510 *et seq.*, and committed the common law tort of "intrusion upon seclusion" in violation of Maryland law. Ethiopia has appeared, but moves to dismiss on numerous grounds.

As explained below, the Court concludes that the Wiretap Act does not create a private cause of action against a foreign state and that the plaintiff's state-law tort claim is barred by the Foreign Sovereign Immunities Act ("FSIA"), 28 U.S.C. §§ 1602–1611. The Court, accordingly, **GRANTS** Ethiopia's motion and dismisses the amended complaint.

I. BACKGROUND

For present purposes, the Court accepts at true the allegations of the amended complaint, along with the incorporated material.[1] *See Price v. Socialist People's Libyan Arab Jamahiriya*, 294 F.3d 82, 93 (D.C. Cir. 2002) (when reviewing "a plaintiff's unchallenged factual allegations to determine whether they are sufficient to deprive a foreign state defendant of sovereign immunity, [the court must] assume those allegations to be true" (citations omitted)); *Gordon v. United States Capitol Police*, 778 F.3d 158, 163–64 (D.C. Cir. 2015) (under Federal Rule of Civil Procedure 12(b)(6), the court "must accept the complaint's allegations as true and draw all reasonable inferences in favor of the non-moving party").

Plaintiff John Doe, who uses the pseudonym "Kidane" in connection with his political activities, is a U.S. citizen who was born in Ethiopia and has lived in the United States since obtaining asylum in the early 1990s. Dkt. 1-1 ¶ 3; Dkt. 26 at ¶¶ 3, 19, 20. At all relevant times, Kidane resided in Silver Spring, Maryland, where he has remained active "within the Ethiopian Diaspora." Dkt. 26 ¶¶ 19, 20. He asserts that "the Ethiopian government monitors political dissidents at home and abroad . . . through the use of electronic surveillance," *id.* ¶ 25, and that he was subjected to such surveillance by means of a program secretly installed on his personal computer, controlled by the Ethiopian government or its agents, and used by them to monitor and record his computer activities and communications. *See id.* ¶¶ 3, 5, 9.

[1] Had Ethiopia presented evidence disputing the "factual underpinnings of" Kidane's invocation of an exception to the FSIA, the Court would have been required to "go beyond the pleadings and [to] resolve any disputed issues of fact the resolution of which is necessary to a ruling upon the motion to dismiss." *Phoenix Consulting v. Republic of Angola*, 216 F.3d 36, 40 (D.C. Cir. 2000). But, because Ethiopia has not done so, the Court must resolve Ethiopia's motion based on the facts as alleged.

According to the complaint, in late 2012 or early 2013, Kidane's personal computer, located at his home in Maryland, "bec[a]me infected with clandestine computer programs known as FinSpy." *Id.* ¶ 4. FinSpy is "a system for monitoring and gathering information from electronic devices, including computers and mobile phones, without the knowledge of the device's user." *Id.* ¶ 6. It is allegedly "sold exclusively to government agencies and is not available to the general public." *Id.*; *see also id.*, Ex. A (describing the FinSpy product). Kidane attributes the FinSpy infection of his computer to an email "sent by or on behalf of Ethiopia that was thereafter forwarded to" him by a third party. *Id.* ¶ 5. The complaint does not state where the original third-party recipient was located; Ethiopia argues, however, that the content of the email, which is appended to the complaint, suggests that the original recipient may have resided in London. *See id.*, Ex. C (translation stating, in part, "[y]ou took your family to London . . . ."). In any event, Kidane does not allege or argue that Ethiopia sent the email directly to him or to anyone else located in the United States.

The email contained a Trojan Horse attachment that "trick[ed]" Kidane into opening it, Dkt. 26 ¶¶ 38, 41, "caus[ing] a clandestine client program to be surreptitiously downloaded onto his computer," *id.* ¶ 5, and resulting in the installation of the FinSpy software, *id*. The FinSpy software allegedly "took what amounts to complete control over the operating system" of his computer. *Id.* According to the complaint, FinSpy contains "modules" for "extracting saved passwords from more than 20 different" programs, "for . . . recording Internet telephone calls, text messages, and file transfers transmitted through the Skype application," "for covertly recording audio from a computer's microphone even when no Skype calls are taking place," "for recording every keystroke on the computer," and "for recording a picture of the contents displayed on a computer's screen." *Id.* ¶ 36–37.

Kidane alleges that once FinSpy infected his computer, it "began contemporaneously recording some, if not all, of the activities undertaken by users of the computer, including [Kidane] and members of his family." *Id.* He alleges that it "surreptitiously intercepted and contemporaneously recorded dozens of [his] private Skype Internet phone calls, recorded portions or complete copies of a number of [his] emails," and copied a web search conducted by his son for a ninth-grade research assignment. *Id.* ¶ 3. He further avers that evidence of these activities was found in various "FinSpy trace files" on his computer. *See id.* ¶¶ 55–60, 64–77. These trace files included, for example, "files consistent with FinSpy's naming convention [that] contain portions or complete copies of [Kidane's] private and highly confidential Skype conversations." *Id.* ¶ 69.

Kidane further alleges that the FinSpy software installed on his computer communicated with a computer server located in Ethiopia. *Id.* ¶ 10. As explained in the complaint and attached exhibits, computers that have been infected with the FinSpy software typically communicate with a designated "FinSpy Master" server via a "FinSpy Relay." *Id.* ¶¶ 35, 43–51, Ex. A. The "FinSpy Master" determines whether, under the applicable FinSpy license terms, a given copy of the software will be activated. *Id.* ¶¶ 44–45, Ex. A. Once the software is activated, the FinSpy Master "sends commands to [the] infected device[] and receives gathered information" from that device. *Id.* ¶ 35. According to a report attached to the complaint, "a recently acquired [FinSpy] malware sample" shows that the malware has used "images of members of the Ethiopian opposition group, Ginbot 7, as bait, and that it has communicated with a FinSpy Command & Control server in Ethiopia." Dkt. 26, Ex. B. In particular, the malware communications "can be found in [an] address block run by Ethio Telecom, Ethiopia's state owned telecommunications provider." *Id.* Kidane alleges that "the FinSpy Relay and FinSpy Master servers with which

[his] computer in Maryland was controlled are located inside Ethiopia and controlled by Defendant Ethiopia," *id.* ¶ 85, and that the FinSpy installation "took instructions from a FinSpy relay controlled by Defendant Ethiopia," *id.* ¶ 84. He further alleges that FinSpy, but not all of the distinct trace files, "appears to have been removed" from his computer just five days after the publication of a report that disclosed "the technical details of the FinSpy Relay" used by Ethiopia. *Id.* ¶ 77.

The complaint contains two counts: a claim under the Wiretap Act, alleging that Ethiopia illicitly intercepted Kidane's Skype calls and "other data," *id.* ¶¶ 92–100, and a claim under Maryland tort law for intrusion upon seclusion, alleging that Ethiopia unlawfully monitored and recorded Kidane's and his family's private computer activities, including Skype calls, emails, and web searches, *id.* ¶¶ 101–105. Citing a fear of retaliation against himself and his family members in the United States and Ethiopia, Kidane moved for leave to proceed pseudonymously—as either John Doe or using the name "Kidane." *See* Dkt. 1-1 at 11–13. The Court granted that motion. *See* Dkt. 2.

Ethiopia moved to dismiss the complaint, *see* Dkt. 27, and, after the matter was fully briefed, the Court held oral argument on Ethiopia's motion. In light of the fact that the case presents "substantial issues relating to the interpretation and application of the Foreign Sovereign Immunities Act's non-commercial tort exception, 28 U.S.C. § 1605(a)(5), including the discretionary function exception and the 'entire tort' rule," the Court then provided the United States with the opportunity to file a brief. *See* Dkt. 35. The United States responded that it was "actively considering whether to file a Statement of Interest as permitted by 28 U.S.C. § 517," and requested additional time to "complete its deliberations," and, if appropriate, to file a

Statement of Interest. Dkt. 37. The United States ultimately declined, however, to file a brief at this stage of the proceeding. Dkt. 38.

II. ANALYSIS

Ethiopia moves to dismiss on multiple grounds, contending both that this Court lacks jurisdiction under the FSIA and that Kidane fails to state a claim under the Wiretap Act because the Act does not provide a cause of action against a foreign state. *See* Dkt. 27. In the ordinary course, the Court would start with the jurisdictional question, because jurisdiction is a precondition to the Court's "power to declare the law, and when it ceases to exist, the only function remaining to the court is that of announcing the fact and dismissing the cause." *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94 (1998) (quoting *Ex parte McCardle*, 74 US (7 Wall) 506, 514 (1868)).

In *Vermont Agency of Natural Resources v. United States ex rel. Stevens*, 529 U.S. 765 (2000), however, the Supreme Court recognized a narrow exception to this rule. There, as here, the Court possessed Article III jurisdiction but was called upon to decide whether sovereign immunity—there, the Eleventh Amendment immunity of the state of Vermont—barred the action. *Id.* at 778. Before resolving that jurisdictional question, however, the Court concluded that it was appropriate to consider whether the relevant statute "permit[ed] the cause of action [Congress] create[d] to be asserted against States." *Id.* at 779. As the Supreme Court explained, "[w]hen . . . two questions [of this sort] are at issue, not only is the statutory question 'logically antecedent to the existence of' the . . . question" of sovereign immunity, "but also there is no realistic possibility that addressing the statutory question will expand the Court's power beyond the limits that the jurisdictional restriction has imposed." *Id.*

The same is true with respect to Kidane's claim under the Wiretap Act. The question

whether Congress intended to subject foreign sovereigns to suit under the Wiretap Act is antecedent to the question whether Ethiopia would, under the FSIA, be immune from suit for any such violation. As in *Vermont Agency of Natural Resources*, moreover, resolving the statutory question first does not risk expanding the Court's power beyond the jurisdictional limits prescribed by Congress; indeed, both the statutory and jurisdictional issues pose essentially the same question—did Congress intend to subject foreign states to suit in U.S. courts under the Wiretap Act? The Court, accordingly, starts with the question whether the Wiretap Act applies to foreign states before turning to the application of the FSIA.

A. Applicability of the Wiretap Act to Foreign States

The Wiretap Act imposes criminal penalties and establishes a private cause of action for, among other things, the unauthorized interception of "any wire, oral, or electronic communication." 18 U.S.C. § 2511(1) (liability); *see also id.* §§ 2511(4) (criminal penalties), 2520(a) (private cause of action for civil damages). According to Ethiopia, however, the Wiretap Act does not apply to foreign states. That contention raises two distinct questions: First, does the *prohibition* on unauthorized interception of communications contained in section 2511(1) of the Wiretap Act apply to governmental entities? Second, if not, does the civil *cause of action* created in the Act nonetheless authorize private litigants to sue governmental entities, including foreign states, for violations of section 2511(1)?

As usual, the Court "begin[s] with the text of the statute." *Kasten v. Saint-Gobain Performance Plastics Corp.*, 563 U.S. 1, 7 (2011). The prohibition of the Wiretap Act at issue in this case is found in section 2511(1)(a), which makes it a crime for "any person" to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept . . . any wire, oral, or electronic communication" without lawful authorization. The term "person,"

in turn, is defined 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.* § 2510(6). Thus, by its plain terms, the prohibition in section 2511(1)(a) does not apply to governmental entities; rather, it is limited to suits against those acting on behalf of the United States and state and local governments, other individuals, and various non-governmental entities. That reading of the statute is consistent, moreover, with the "longstanding interpretative presumption that 'person' does not include the sovereign," *Vermont Agency of Nat'l Res.*, 529 U.S. at 780, and with the legislative history of the Wiretap Act, which indicates that even though the "definition [of 'person'] explicitly includes any officer or employee of the United States or any State or political subdivision of a State," it excludes "the governmental units themselves," S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2179. The Court, accordingly, concludes that the prohibition on unauthorized interception of wire, oral, or electronic communications contained in section 2511(1)(a) does not apply to governmental entities, much less foreign states.

Kidane does not resist this line of reasoning, but instead argues that two amendments to the provision of the Wiretap Act establishing a private cause of action for civil damages, section 2520, opened the door to private suits against governmental entities, including foreign states, for violations of section 2511(1)(a) of the Act. As originally enacted in 1968, section 2520 provided a cause of action for a "person whose wire or oral communication is intercepted . . . in violation of this chapter . . . against *any person* who intercepts . . . such communications." *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, § 802, 82 Stat. 213 (1968) (emphasis added). In 1986, however, Congress enacted the Electronic Communications Privacy Act ("ECPA"), which—along with a more comprehensive overhaul of the privacy laws

to address electronic communications—modified section 2520 to permit recovery "from the person *or entity* which engaged in that violation [of this chapter]." Pub. L. No. 99-508, Title I, § 103, 100 Stat. 1848 (1986) (emphasis added). Then, in 2001, Congress again amended section 2520 in the PATRIOT Act. That amendment changed the relevant language to its current form, which provides that a person who has been subjected to the unlawful interception of his wire, oral, or electronic communications may sue "the person or entity, *other than the United States*, which engaged in that violation." Pub. L. No. 107-56, Title I, § 223, 115 Stat. 293, 384 (2001) (codified at 18 U.S.C. § 2520(a) (2012)) (emphasis added).

As Kidane correctly observes, the phrase "or entity" in section 2520(a) "logically must refer to [at least some] governmental entities in order to have meaning and effect." Dkt. 28 at 19. A number of courts considering claims against local governments have so held.[2] As they explain, "[t]he addition of the words '[or] entity' can only mean a governmental entity because prior to the 1986 amendments, the definition of 'person' already included business entities. In order for [the addition of] the term ['entity' to section 2520] not to be superfluous, the term 'entity' [must] mean[] governmental entities." *Adams*, 250 F.3d at 985. In addition, although there is no legislative history discussing ECPA's addition of the phrase "or entity" to section 2520, ECPA simultaneously "added the same language to the civil liability provision for

[2] *See Adams v. City of Battle Creek*, 250 F.3d 980, 985–86 (6th Cir. 2001); *Garza v. Bexar Metro. Water Dist.*, 639 F. Supp. 2d 770, 773–75 (W.D. Tex. 2009); *Williams v. City of Tulsa*, 393 F. Supp. 2d 1124, 1132 (N.D. Okla. 2005); *Conner v. Tate*, 130 F. Supp. 2d 1370, 1373–74 (N.D. Ga. 2001); *Dorris v. Absher*, 959 F. Supp. 813, 820 (M.D. Tenn. 1997), *aff'd in part, rev'd in part on other grounds*, 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); *Bodunde v. Parizek*, No. 93-1464, 1993 WL 189941, at *3–4 (N.D. Ill. May 28, 1993); *Huber v. N. Carolina State Univ.*, 594 S.E.2d 402, 407 (N.C. 2004). *See also Organizacion JD Ltda. v. U.S. Dep't of Justice*, 18 F.3d 91, 95 (2d Cir. 1994) (holding parallel cause of action in section 2707 for violations of the Stored Communications Act covers municipality). The D.C. Circuit has not addressed the issue.

interception of stored wire and electronic communications" contained in 18 U.S.C. § 2707 (Stored Communications Act). *Id.* "The Senate [and House] Committee Report[s] summarizing [section] 2707, the parallel section for liability for intercepting stored communications, specifically state[] that the word 'entity' includes governmental entities." *Id.*; *see also* S. Rep. No. 99-541, at 43 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3597; H.R. Rep. No. 99-647 at 74 (1986). If ECPA's addition of the word "entity" to section 2707 included "governmental entities," Kidane posits that the same must be true for ECPA's addition of the same language to section 2520.

The 2001 amendment to section 2520 contained in the PATRIOT Act, likewise, supports the conclusion that at least some governmental entities are subject to suit for violating at least certain provisions of the Wiretap Act. The addition of the phrase "other than the United States" as a modifier of the word "entity" in section 2520(a) confirms that "entity" must cover some governmental bodies. *See Garza*, 639 F. Supp. 2d at 775; *Williams*, 393 F. Supp. 2d at 1132; *Huber*, 594 S.E.2d at 407. Although "[w]hat limited legislative history exists is silent on the addition of this language," *Williams*, 393 F. Supp. 2d at 1132-33, the phrase "other than the United States" would have been unnecessary unless Congress understood the preceding term "entity" otherwise to encompass governmental entities. *See id.*; *Garza*, 639 F. Supp. 2d at 775; *Huber*, 594 S.E.2d at 407.

For these reasons, the Court does not doubt that the term "entity," as used in section 2520, refers to at least some governmental entities for some purposes. *See also Seitz v. City of Elgin*, 719 F.3d 654, 657–60 (7th Cir. 2013) ("The plain meaning of 'entity' includes government units."). But that does not answer the question whether Congress intended to expose those entities to suits for violations of section 2511(1)(a) in particular, as opposed to suits for

violations of other prohibitions in the Wiretap Act. Many courts considering claims against local governments have assumed the former, without elaboration.[3] But, as explained above, the plain language of section 2511(1)(a) applies only to "persons," and that phrase is defined in a manner that does not include governmental entities.

The courts that hold that the amendments to section 2520 permit a civil action against local governmental entities for a violation of section 2511(1) treat those amendments as implicitly amending the definition of "person" and the scope of section 2511(1). *See supra* n.3. That conclusion turns on the premise that the phrase "person or entity, other than the United States" makes sense only if section 2511(1) is construed to reach the conduct of governmental "entities" "other than the United States." That is, although "[s]ection 2520 itself creates no substantive rights," *Seitz*, 719 F.3d at 657, many courts assume that the amendments to section 2520 covering governmental entities can be given meaning only if they are construed to have imposed a corresponding duty on governmental entities under section 2511(1) not to unlawfully intercept, endeavor to intercept, or procure another person to intercept communications.

The problem with this argument is that it is not at all difficult to give meaning to Congress's creation of a cause of action against governmental entities other than the United States without expanding the scope of section 2511(1) or implicitly amending the statutory definition of "person" to include governmental entities. As the Seventh Circuit has explained, at the same time that Congress added the phrase "or entity" to section 2520, it also added section 2511(3)(a) to the Wiretap Act. *See Seitz*, 719 F.3d at 659. Like section 2511(1), that section

---

[3] *See Adams*, 250 F.3d at 985–86; *Garza*, 639 F. Supp. 2d at 773–75; *Williams*, 393 F. Supp. 2d at 1132; *Conner*, 130 F. Supp. 2d at 1373–74; *Dorris*, 959 F. Supp. at 820; *PBA Local No. 38*, 832 F. Supp. at 823; *Bodunde*, 1993 WL 189941, at *3–4; *Huber*, 594 S.E.2d at 407. *But see Seitz*, 719 F.3d at 657–60.

prohibits specified conduct but, unlike section 2511(1), it applies to any "person *or entity*." *Id.* (emphasis added). In particular, with certain exceptions, section 2511(3)(a) prohibits "*a person or entity* providing an electronic communication service to the public [from] intentionally divulg[ing] the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication." 18 U.S.C. § 2511(3)(a) (emphasis added). It is thus not surprising that, at the same time that Congress added this prohibitory language to the statute, it also amended section "2520 to match the 'person or entity' language used in [section] 2511(3). Without that change, parties could sue a 'person' who violated [section] 2511(3)(a) but not an entity even though [section] 2511(3) explicitly referenced both." [4] *Seitz*, 719 F.3d at 658–59 (internal footnotes and citation omitted). *See also Adams v. Luzerne Cty.*, 36 F. Supp. 3d 511, 523 (M.D. Pa. 2014); *Whitaker v. Barksdale Air Force Base*, No. 14-2342, 2015 WL 574697, at *5 (W.D. La. Feb. 11, 2015); *Anderson v. City of Columbus, Georgia*, 374 F. Supp. 2d 1240, 1244–46 (M.D. Ga. 2005). As a result, the Court can give sections 2510(6) and 2511(1) their plain meaning, while also "giv[ing] meaning to each word of [section] 2520[(a)]." *Seitz*, 719 F.3d at 658.

Kidane might, instead, be understood to contend that, even if Congress did not expand the scope of sections 2510(6) and 2511(1) through the amendments to section 2520, it amended section 2520 to create a cause of action against a *government* for substantive violations of section 2511(1) committed by *individuals* acting on behalf of that state—based, for example, on *respondeat superior* liability. Under this theory, even though a foreign government is not itself

[4] Although section 2511(3)(a) addresses "person[s]" or "entit[ies]" who provide "an electronic communication service to the public," the provision is not limited to the regulation of *private* enterprise. "Apparently, municipal governments have, in fact, entered or attempted to enter the telecommunications business." *Seitz*, 719 F.3d at 659.

subject to section 2511(1), it may be vicariously liable for violations of section 2511(1) committed by its agents, who are "individuals" and thus arguably "persons" as defined in section 2510(6).

This argument, however, cannot be squared with the text of the Wiretap Act for two reasons. First, section 2520 permits a party whose communications were unlawfully intercepted to "recover from *the person or entity*, other than the United States, *which engaged in that violation*." 18 U.S.C. § 2520(1) (emphases added). Accordingly, the "person or entity" subject to suit must be the same "person or entity" that violated the statute. Second, permitting suit against a governmental entity that could not itself "engage[] in" a violation of section 2511(1) is also at odds with the statutory definition of "person" contained in section 2510(6). In that definition, Congress defined the specific types of juridical bodies capable of violating section 2511(1) to include a "partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6). Because these entities can act only through their members, agents, officers, and employees, the definition necessarily already encompasses a concept of agent-principal or vicarious liability. To graft yet an additional theory of such liability onto section 2520 would undermine the balance that Congress struck. *Cf. Cicippio-Puleo v. Islamic Republic of Iran*, 353 F.3d 1024, 1036 (D.C. Cir. 2004) (declining to imply cause of action against foreign government where "the liability imposed by [28 U.S.C. § 1605(a)(7)] is precisely limited to 'an official, employee, or agent of a foreign state designated as a state sponsor of terrorism'").

The Court, accordingly, concludes that section 2520 of the Wiretap Act does not create a civil cause of action against a foreign state for interceptions of wire, oral, or electronic communications in violation of section 2511(1), and thus **GRANTS** Ethiopia's motion to dismiss Count One of the complaint.

B. Foreign Sovereign Immunities Act

The conclusion that Congress did not create a private cause of action against foreign states for violations of section 2511(1) of the Wiretap Act does not resolve the case, because Kidane also asserts a claim based on the common law tort of intrusion upon seclusion. *See* Dkt. 26 ¶¶ 101–05. Under Maryland law, this tort requires "the intentional intrusion upon the solitude or seclusion of another or his private affairs or concerns [in a manner] that would be highly offensive to a reasonable person." *Pemberton v. Bethlehem Steel Corp.*, 502 A.2d 1101, 1116 (Md. Ct. Spec. App. 1986) (citing Restatement (Second) of Tort, § 652B (1977)). The question remains whether the FSIA bars Kidane from asserting this claim against Ethiopia.

Although the FSIA was not enacted until 1976, foreign sovereign immunity dates back to the earliest days of the Republic. *See Verlinden B.V. v. Central Bank of Nigeria*, 461 U.S. 480, 486 (1983). Originally, the United States accorded foreign states absolute immunity from suit in its courts. *See* Restatement (Third) of the Foreign Relations Law of the United States, ch. 5, subch. A, intro. n. (1987 & 2016 Supp.) ("Until the twentieth century, sovereign immunity from the jurisdiction of foreign states seemed to have no exceptions."); *see also Republic of Mexico v. Hoffman*, 324 U.S. 30, 35 (1945); *The Schooner Exchange v. M'Faddon*, 11 U.S. (7 Cranch) 116, 136–37, 146 (1812). Beginning in the 1950s, however, the United States adopted the "restrictive" theory of sovereign immunity under which "sovereign or public actions" of a state are immunized, but "private acts" are not. *See* Letter from Jack B. Tate, Acting Legal Adviser, U.S. Dep't of State, to Philip B. Perlman, Acting Attorney Gen., *reprinted in Alfred Dunhill of London, Inc. v. Cuba*, 425 U.S. 682, 711–715 (1976). In the State Department's view, absolute foreign sovereign immunity had become "inconsistent with the action of the Government of the United States in subjecting itself to suit in these same courts in both contract and tort," and "the

widespread and increasing practice on the part of governments of engaging in commercial activities [made] necessary a practice which will enable persons doing business with them to have their rights determined in the courts." *Id.* at 714.

Almost a quarter-century later, Congress enacted the FSIA, which, with modest refinements, codified the restrictive theory of immunity. *See Verlinden*, 461 U.S. at 488. Since its enactment, the FSIA has "provide[d] 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, 434 (1989). The Act provides a foreign state with "'presumptive[] immun[ity] from the jurisdiction of United States courts' unless one of the Act's express exceptions to sovereign immunity applies." *OBB Personenverkehr AG v. Sachs*, 136 S.Ct. 390, 394 (2015) (quoting *Saudi Arabia v. Nelson*, 507 U.S. 349, 355 (1993)); *see also* 28 U.S.C. § 1604. "When one of [the] . . . specified exceptions applies," however, "'the foreign state [is] liable in the same manner and to the same extent as a private individual under like circumstances.'" *Verlinden*, 461 U.S. at 488–89 (quoting 28 U.S.C. § 1606).

Kidane invokes only one exception to the FSIA—the non-commercial tort exception. *See* Dkt. 26 ¶ 14. That exception to sovereign immunity applies to any case "not otherwise encompassed by" the commercial-activity exception

> 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). There are two statutory "exceptions to the [non-commercial tort] exception," *MacArthur Area Citizens Ass'n v. Republic of Peru*, 809 F.2d 918, 921 (D.C. Cir. 1987), *modified in other respects by* 823 F.2d 606 (D.C. Cir. 1987), both of which parallel

similar provisions in the Federal Torts Claims Act ("FTCA"). The first, known as the discretionary function exception, provides that a foreign state's immunity is not waived with respect to "any claims based upon the exercise [of] a discretionary function." *See* 28 U.S.C. § 1605(a)(5)(A). The second, known as the intentional tort exception, provides that immunity is not waived for claims alleging specified intentional torts, including "misrepresentation" and "deceit." *See id.* § 1605(a)(5)(B).

Ethiopia contends that the non-commercial tort exception to immunity is inapplicable for four reasons: First, it argues that the complaint fails to identify any tortious conduct engaged in by an agent of Ethiopia while in the United States and that the tort, therefore, did not "occur[] in the United States" within the meaning of the exception. Second, it contends that, even if taken as true, Kidane's allegations involve the type of conduct "grounded in social, economic, and political policy" that the discretionary function exception immunizes from suit. *See United States v. Varig Airlines*, 467 U.S. 797, 814 (1984). Third, it maintains that the alleged surreptitious infection of Kidane's computer involves "misrepresentation" and "deceit" and that the intentional tort exception to the non-commercial tort exception therefore applies. Finally, it argues that Kidane has not alleged with sufficient specificity a claim for "money damages . . . for personal injury," as required to fall within the non-commercial tort exception. As explained below, although the Court is unconvinced by three of Ethiopia's arguments, it agrees that Kidane's claim for intrusion upon his seclusion is barred by sovereign immunity because the "entire tort" was not committed in the United States.

1. *The Personal Injury Requirement and the Intentional Tort Exception*

The Court disposes of Ethiopia's third and fourth contentions first, as they require only brief discussion. According to Ethiopia, Kidane's claim for intrusion upon seclusion does not

seek "money damages . . . for personal injury" as required to invoke the non-commercial tort exception because the operative complaint contains only a conclusory allegation that Kidane suffered "emotional distress" as a result of Ethiopia's alleged surveillance. Dkt. 27-2 at 23. Ethiopia stresses that Kidane's original complaint did not include this allegation and argues that the amended complaint's addition of the "bald assertion that [Kidane] suffered personal injury or emotional distress" does not clear the pleading hurdle established in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007). Dkt. 27-2 at 23.

The Court disagrees. *Iqbal* and *Twombly* require only that a plaintiff allege a claim with sufficient factual specificity that it is "plausible on its face." *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570). Here, it is certainly plausible that an asylee would suffer emotional distress upon learning that the foreign state from which he fled was surreptitiously intercepting and recording his (and his family's) Skype calls, email communications, and web searches. Dkt. 26 ¶ 4. And the fact that Kidane did not allege that he suffered emotional distress in his original complaint does not mean that the allegation of emotional distress included in his amended complaint should be greeted with skepticism, as Ethiopia suggests. Rather, at this stage of the proceeding, and in light of the fact that Ethiopia has not introduced any controverting evidence, the Court must take all plausible allegations contained in the operative complaint as true. *See Gordon*, 778 F.3d at 163–64; *Price*, 294 F.3d at 93.

Ethiopia's contention that it is immune from liability for its alleged intrusion upon Kidane's intrusion under the intentional tort exception is equally flawed. *See* Dkt. 27-2 at 13. The intentional tort exception renders the non-commercial tort exception inapplicable to claims "arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights." 28 U.S.C. § 1605(a)(5)(B). It is true that Kidane alleges

that Ethiopia used trickery to place the FinSpy malware on his computer. But neither misrepresentation nor deceit is an element of the tort of intrusion upon seclusion under Maryland law. *See Pemberton*, 502 A.2d at 1116. It is the unreasonable invasion of a plaintiff's privacy that forms the core of the tort, and privacy torts are not among those enumerated in the intentional tort proviso to the non-commercial tort exception. *See* 28 U.S.C. § 1605(a)(5)(B). "Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent." *Andrus v. Glover Const. Co.*, 446 U.S. 608, 616–17 (1980). The omission of privacy torts from the intentional tort exception to the non-commercial tort exception is thus dispositive.

The D.C. Circuit reached precisely this conclusion in a decision interpreting the FTCA's analogous intentional tort exception. *See Black v. Sheraton Corp. of Am.*, 564 F.2d 531, 539 (D.C. Cir. 1977) (interpreting 28 U.S.C. § 2680). In that case, a lobbyist affiliated with Bobby Baker, a long-time advisor to Lyndon Johnson, brought suit alleging that the government had illegally eavesdropped on his conversations by installing a microphone in the wall of his hotel room. *Id.* at 534–35. Rejecting an argument similar to Ethiopia's, the Court of Appeals held that "because invasion of privacy does not fall within an enumerated [intentional tort] exemption [in the FTCA], such a claim is not barred by the doctrine of governmental immunity." *Id.* at 539 n.3; *see also Cruikshank v. United States*, 431 F. Supp. 1355 (D. Haw. 1977). That same conclusion applies with equal force in the present context. Kidane's intrusion upon seclusion claim is not among the enumerated intentional torts that fall outside the non-commercial tort exception. And the mere fact that the allegedly illegal surveillance was conducted surreptitiously is insufficient to bar his claim.

2. *Whether the Tort "Occur[ed] in the United States"*

Whether the alleged intrusion upon Kidane's intrusion "occur[ed] in the United States" within the meaning of the non-commercial tort exception is a much closer question. Although it is well-settled that the non-commercial tort exception "covers only torts occurring within the territorial jurisdiction of the United States," *Amerada Hess Shipping Corp*., 488 U.S. at 441, it is unclear how that rule applies to the instant case, in which the alleged intrusion involves the infiltration of Kidane's computer located at his home in Maryland, yet no agent or employee of Ethiopia is alleged to have ever set foot in the United States in connection with that tort.

On its face, the non-commercial tort exception merely asks whether the suit is for "money damages . . . 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." 28 U.S.C. § 1605(a)(5) (emphasis added). Courts, however, have repeatedly interpreted the phrase "occurring within the United States" to mean that the "entire tort" must have occurred in the United States. *See, e.g., Jerez v. Republic of Cuba*, 775 F.3d 419, 424 (D.C. Cir. 2014); *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1525 (D.C. Cir. 1984); *O'Bryan v. Holy See*, 556 F.3d 361, 382 (6th Cir. 2009); *Von Dardel v. USSR*, 736 F. Supp. 1, 7 (D.D.C. 1990). Under these cases, the fact that the plaintiff incurred an *injury* in the United States, or that the "alleged tort may have had *effects* in the United States," is insufficient to waive sovereign immunity. *Amerada Hess Shipping Corp.*, 488 U.S. at 441 (emphasis added). Rather, "not only the injury but also the act precipitating that injury . . . must occur in the United States." *Jerez*, 775 F.3d at 424; *see also Persinger v. Islamic Republic of Iran*, 729 F.2d 835, 842 (D.C. Cir. 1984) ("[B]oth the tort and the injury must occur in the United States.").

As other courts have explained, this conclusion follows from both the text and legislative history of the FSIA. As a textual matter, the language of the non-commercial tort exception, which includes the "occurring in the United States" requirement, stands in marked contrast to the language of the commercial tort exception, which applies to conduct "'outside the territory of the United States' having a 'direct effect' inside the United States." *Amerada Hess Shipping Corp.*, 488 U.S. at 441 (quoting 28 U.S.C. § 1605(a)(2)).[5] And the legislative history confirms that the non-commercial tort exception applies only to torts occurring in the United States. "Congress' primary purpose in enacting [section] 1605(a)(5) was to eliminate a foreign state's immunity for traffic accidents and other *torts committed in the United States*, for which liability is imposed under domestic tort law." *Id.* at 439–40 (emphasis added). Both the committee reports and the proponents of the legislation repeatedly emphasized that liability would be limited to torts committed within the United States. *See* H.R. Rep. No. 94-1487, at 21, *reprinted in* 1976 U.S.C.C.A.N. 6604 ("[T]he tortious act or omission must occur within the jurisdiction of the United States."); S. Rep. No. 94-1310, at 20 (1976) (same); *Hearing on H.R. 3493 Before the Subcomm. on Claims & Gov't Relations of the H. Comm. on the Judiciary,* 93d Cong., at 21 (1973) ("1973 Hearing") (statement of Charles N. Brower, Acting Legal Adviser, Dep't of State) (although "cast in general terms," the exception was "directed primarily to the problem of traffic accidents," and was intended to apply only to tort claims where "the negligent or wrongful act

[5] Neither party cites any decisions applying the FSIA's non-commercial tort exception to torts facilitated by the Internet and directed from abroad. At least one court has held that the FSIA's commercial tort exception, 28 U.S.C. § 1605(a)(2), waives sovereign immunity for acts perpetrated over the Internet by a foreign state. *See CYBERsitter, LLC v. P.R.C.*, 805 F. Supp. 2d 958, 975 (C.D. Cal. 2011) (holding that claims based on the misappropriation of plaintiff's software and its placement on the foreign state's website fell within the commercial tort exception). But decisions applying the commercial tort exception are inapplicable here because, as explained above, that exception applies to claims based on an extraterritorial act that "causes a *direct effect* in the United States." 28 U.S.C. § 1605(a)(2) (emphasis added).

took place in the United States"); *see also* 1973 Hearing at 34 (letter from Richard G. Kleindienst, Attorney Gen., & William P. Rogers, Sec'y of State); 1973 Hearing at 42 (section-by-section analysis).

Here, it is undisputed that the alleged injury to Kidane occurred in the United States. Ethiopia and Kidane propound very different theories, however, regarding where the allegedly tortious act or acts occurred, each of which has some merit and neither of which wholly resolves the question.

According to Ethiopia, accepting the allegations of the complaint as true, "the *acts* underlying the tort, as distinct from their alleged *injurious effect*, occurred overseas." Dkt. 27-2 at 16 (emphases added). Ethiopia focuses on the fact that "[t]he actors who committed the alleged tort, according to Plaintiff, were operating in Ethiopia, the computer servers were located in Ethiopia, the spyware was maintained in Ethiopia, the commands came from Ethiopia, and Plaintiff's materials were viewed in Ethiopia." Dkt. 27-2 at 11; *see also id.* at 9–11. In its view, "inasmuch as both the acts and intent occurred overseas, the two alleged intentional torts have their *situs* overseas and therefore, by definition did not occur entirely in the United States." *Id.* at 17. Thus, according to Ethiopia, the location of the alleged tort—or at least a substantial portion of it—was overseas because all of the alleged tortfeasors were located overseas and it is *their* extraterritorial conduct that allegedly precipitated Kidane's injury.

Although not without some force, this argument is incomplete because it fails to grapple with the modern world in which the Internet breaks down traditional conceptions of physical presence. Thus, while the Congress that enacted the FSIA in 1976 envisioned the paradigmatic case for liability as involving an embassy employee who causes an automobile accident while on official business in the United States, *see, e.g.*, H.R. Rep. No. 94-1487, at 29, we now live in an

age where, according to press reports, it is possible to hack remotely into a car's electronics and to cause the same crash from thousands of miles away.[6] Here, as Kidane points out, Ethiopia's alleged surveillance would fall squarely within the "entire tort" rule had it sent a "flesh-and-blood agent into [Kidane's] house to install a recording device." Dkt. 28 at 27. Technology has simply rendered the human agent obsolete.

Kidane's theory of where the tortious conduct occurred, in contrast, focuses not on the physical location of the tortfeasor, but on the elements of the state law cause of action, asserting that "every element of the asserted claim occurred in the United States—from the installation of spyware on a U.S. computer, to the interception of electronic communications." Dkt. 28 at 23. As Kidane correctly points out, under Maryland law, "the gravamen of the tort [of intrusion upon seclusion] is the intrusion into a private place or the invasion of a private seclusion that the plaintiff has thrown about his person or affairs." Dkt. 28 at 24 (quoting *New Summit Assocs. Ltd. P'ship v. Nistle*, 533 A.2d 1350, 1354 (Md. Ct. Spec. App. 1987)). A plaintiff, moreover, need not allege that a physical trespass occurred to state a claim for intrusion upon seclusion. *See Pearson v. Dodd*, 410 F.2d 701, 704 (D.C. Cir. 1969). And, although no decision from the Maryland courts has addressed the issue to date, the Court can assume for present purposes that the mere "tapping" or "bugging" of personal communications is sufficient to state a claim, even if no one ever listens to the plaintiff's communications. *See Hamberger v. Eastman*, 206 A.2d 239, 242 (N.H. 1964) (rejecting contention that plaintiffs failed to state a claim for intrusion upon seclusion because "there are no allegations that anyone listened or overheard sounds or

[6] *See* New York Times Bits Blog, *Security Researchers Find A Way To Hack Cars* (July 21, 2015), *available at* http://bits.blogs.nytimes.com//2015/07/21/security-researchers-find-a-way-to-hack-cars/.

voices originating from plaintiffs' bedroom"); *New Summit Assocs. Ltd. P'ship*, 533 A.2d at 1354 ("[P]laintiff was not required to prove that a particular individual actually observed her" through peephole); *Pearson*, 410 F.2d at 704 & nn.10 & 14 (citing *Hamberger* with approval and stating that "[t]he tort is completed with the obtaining of the information by improperly intrusive means").[7] The question for the factfinder, then, is simply whether the defendant intentionally intruded "upon the solitude or seclusion of another or his private affairs or concerns" in a manner that "would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B.

Neither the text of the FSIA nor existing case law clearly resolves whether Ethiopia or Kidane's conception of where the alleged tort occurred for purposes of the non-commercial tort exception is correct, and the question is a close one. Three considerations, however, convince the Court that Ethiopia's view is more compelling:

First, the question of where the "entire tort" occurred cannot be wholly divorced from the physical location of the tortfeasors. Kidane stresses that the tort of intrusion upon seclusion does not require that he prove that Ethiopia ever transferred information from his computer to a computer located in Ethiopia or that anyone in Ethiopia—or anywhere else—actually listened to or read his communications; all that was required was that Ethiopia took control of his computer and caused that computer to make illicit copies of the relevant communications. But that view of where the tort occurred ignores the fact that all of the acts by Ethiopia or its agents that allegedly precipitated the tort occurred outside the United States. *Jerez*, 775 F.3d at 424. The complaint does not suggest that the email containing the malware was prepared in the United States or that

[7] *But see Marks v. Bell Tel. Co. of Pennsylvania*, 331 A.2d 424, 431 (Pa. 1975) ("In the absence of an overhearing of a private communication, this tort has not been committed."); *LeCrone v. Ohio Bell Tel. Co.*, 201 N.E.2d 533, 538 (Ohio Ct. App. 1963) ("[I]n our opinion, the only possible act which could constitute an invasion in the present case is the eavesdropping itself, and the connection or tap here constitutes only a preparation for that invasion of privacy.").

it was sent from within the United States. And, as Ethiopia notes, Kidane does not even allege that anyone acting on behalf of Ethiopia purposefully sent the email to him or to anyone else in the United States; rather, the translation attached to the complaint suggests that the email may have been sent to someone in London, who forwarded it (directly or through others) to Kidane in the United States. Dkt. 26 ¶ 5 & Ex. C. Kidane, moreover, fails to identify any case applying the non-commercial tort exception to circumstances, like those alleged here, where the precipitating acts of the relevant tortfeasor occurred outside the United States. And, although it is also true that no decision has rejected application of the exception in circumstances like those alleged here, courts have at least hinted that the "entire tort" requirement is not satisfied where actions taken outside the United States precipitate events in the United States. *Cf. O'Bryan*, 556 F.3d at 370, 385 (declining to apply non-commercial tort exception to claims attacking a policy against reporting sexual abuse, where the sexual abuse occurred in the United States, but the policy was "presumably" promulgated abroad); *Olsen v. Gov't of Mexico*, 729 F.2d 641, 644, 646 (9th Cir. 1984) (rejecting Mexico's claim of immunity based on fact that airplane was maintained outside the United States where "one entire tort . . .—the negligent piloting of the aircraft—. . . occurred in the United States").

In Kidane's view, little turns on the fact that all of the acts of the alleged tortfeasors occurred overseas. He argues that the D.C. Circuit applies an "essential locus" test, requiring only that "the injury and the act that proximately causes that injury" occur in the United States, and that the acts taken by Ethiopia or its agents that occurred in Ethiopia were merely "collateral" to commission of the alleged tort. Dkt. 28 at 23. Under this theory, the "essential locus" of the tort is Maryland—"where [his] computer was when it was accessed and infected with spyware, and where he was when his communications were intercepted by Ethiopia's

FinSpy device," *id.*—and not Ethiopia—where the tort was allegedly planned and set in motion. Kidane is surely right that the mere fact that "*some* foreign conduct" occurred overseas is insufficient to render a sovereign immune. Dkt. 28 at 26. If that were the case, then an assassination plotted overseas but carried out on American soil would garner immunity, *cf. Letelier v. Republic of Chile*, 488 F. Supp. 665, 673–74 (D.D.C. 1980), and "foreign states [would be encouraged] to allege that some tortious conduct occurred outside the United States," *Olsen*, 729 F.2d at 646.

But, even assuming that the acts that allegedly occurred in Ethiopia were merely "collateral" to the commandeering of Kidane's computer, the Court is unconvinced that the D.C. Circuit has adopted an "essential locus" test. Kidane bases his "essential locus" argument solely on the D.C. Circuit's decision in *Asociacion de Reclamantes v. United Mexican States*. In that case, the Court held that Mexico was immune from a suit challenging its failure to compensate its citizens for land claims it assumed under a treaty with the United States, because the allegedly tortious failure to compensate occurred outside the United States. 735 F.2d at 1524–25. Kidane correctly notes that the Court of Appeals wrote that "[e]ven if the allegedly tortious failure to compensate had the effect of retroactively rendering the prior acts [of entering the treaty] on United States soil tortious, at the very least the entire tort would not have occurred here, and indeed we think its *essential locus* would remain Mexico." *Reclamantes*, 735 F.2d at 1525 (emphasis added). That assertion, however, came only after the Court had already concluded that "the entire tort would not have occurred here," and after it cited with approval the assertion in *In re Sedco, Inc*. that "the tort, *in whole*, must occur in the United States." *Id.* (quoting *In re Sedco, Inc*., 543 F. Supp. 561, 567 (S.D. Tex. 1982)) (emphasis added). The Court's reference to the "essential locus" of the tort, accordingly, was at most an alternative, *a fortioiri* holding. Any

doubt regarding this reading of *Reclamantes*, moreover, is put to rest by subsequent decisions in this jurisdiction that have treated *Reclamantes* as establishing the "clear" rule that "the entire tort" must occur in the United States. *See Jerez*, 775 F.3d at 424; *Von Dardel*, 736 F. Supp. at 7; *see also O'Bryan*, 556 F.3d at 382.

A more recent decision from the D.C. Circuit is arguably more on point, although the Court is also unpersuaded that it vindicates Kidane's position. In *Jerez v. Republic of Cuba*, the plaintiff sought to recover for torture that the Cuban government allegedly inflicted upon him while incarcerated in Cuba, including injecting him with the hepatitis C virus. 775 F.3d at 421. The district court held that Cuba was immune from suit because the "alleged tort . . . occurred in Cuba," and because "none of the defendants . . . was within the United States." *Id.* at 424. On appeal, Jerez argued that "the virus continue[d] to replicate in his body" after he arrived in the United States, and that each replication of the virus constituted a separate tort. *Id.* The D.C. Circuit rejected that argument, holding that the tort occurred in Cuba where Jerez was infected, and that the replication of the virus in the United States merely constituted an ongoing injury—and not a series of new torts. *Id.* But the Court went on to discuss, albeit briefly, how the "entire tort" rule might apply to torts precipitated by acts taken overseas that otherwise occur entirely in the United States. In particular, Jerez argued that his claim was analogous to a claim based on "a foreign agent's delivery into the United States of an anthrax package or a bomb." *Id.*; *see also* Br. for Appellant, at 25, *Jerez v. Republic of Cuba*, 775 F.3d 419 (No. 13-7141), 2014 WL 1713091 (positing hypothetical of anthrax "package that was mailed from abroad"). In response, the Court of Appeals drew a distinction between Jerez's case, in which Cuba's alleged "infliction of injury on Jerez occurred entirely in Cuba," and Jerez's hypotheticals, where "the infliction of injury by the hypothetical anthrax package or bomb would occur entirely in the United States."

775 F.3d at 424.

Although the hypothetical of an anthrax package or bomb mailed from outside the United States is arguably analogous to the sending of malware that infected a computer located in the United States, the Court is leery of reading *Jerez* to provide substantial guidance regarding the application of the non-commercial tort exception to torts committed remotely. Most notably, that is not what was at issue in *Jerez*; to the contrary, the Court of Appeals unambiguously held that the alleged tort "occurred entirely in Cuba," where Jerez was infected with the hepatitis C virus. *Id.* at 421. The fact that the Court went on to distinguish Jerez's hypotheticals on the ground that "the infliction of injury" in the hypothetical occurred entirely in the United States was thus dicta. But, even beyond that, the Court did not conclude that the hypothetical tort would have occurred entirely within the United States, but only that, unlike in Jerez's case, the "injury" would have been "inflicted" in the United States. *Id.*

Second, to the extent that it is uncertain whether Congress intended to permit suit in U.S. courts for torts precipitated from abroad, the D.C. Circuit has cautioned against converting the non-commercial tort exception "into a broad exception for all alleged torts that bear some relationship to the United States." *Reclamantes*, 735 F.2d at 1525. To be sure, the fact that Congress focused on traffic accidents committed by "officials and employees of foreign sovereigns" while "in this country" does not define the full scope of the non-commercial tort exception. *Id*. But it does convey something about the types of tortious conduct that Congress had in mind when it enacted the exception, and the instant allegations are far afield from that paradigmatic case. *Id*. The Court, moreover, must proceed cautiously where application of the exception would arguably shift the balance that Congress struck between the desire to afford members of the public a remedy for torts committed in the United States by foreign employees

and officials and the interest in maintaining comity with foreign states. Applying the exception to torts precipitated exclusively beyond the borders of the United States—by tortfeasors who neither set foot in this Country nor directly caused a tort to be committed here—implicates that balance. As the D.C. Circuit observed in a different context, "[i]f Congress had meant to remove sovereign immunity for governments acting on their own territory, with all of the potential for international discord and for foreign government retaliation that that involves, it is hardly likely that Congress would have ignored those topics and discussed instead automobile accidents in this country." *Persinger*, 729 F.2d at 841.

Put differently, the question whether to afford a foreign state immunity from suit inherently involves a political judgment, raising sensitive issues of foreign relations. When Congress enacted the FSIA, it decided to leave it to the courts to *apply* the rules that the Executive Branch had adopted over many years and that Congress had, with minor adjustment, embodied in the FSIA. But, at the same time, it did not confer common law authority on the courts to *adjust* the rules of foreign sovereign immunity to new and unanticipated events that might arise. To the contrary, the FSIA starts from the premise that foreign states are entitled to immunity, and then carves out limited—and specific—exceptions to that rule. *See* 1973 Hearing at 21 (statement of Charles N. Brower, Acting Legal Adviser, Dep't of State). To the extent that the present dispute seeks to open the door to a new and previously unrecognized class of cases against foreign states made possible by technological changes, that type of judgment is better left to Congress, which has, in fact, amended the FSIA in recent years to address evolving threats—most notably, the emergence of state-sponsored terrorism. *See* Pub. L. No. 110-181, Div. A, Title X, § 1083(a)(1), 122 Stat. 338 (2008) (codified at 28 U.S.C. § 1605A (2012)).

Third, and finally, the legislative history of the non-commercial tort exception, although

limited, provides additional support for the conclusion that Congress did not intend to reach torts precipitated by the actions of tortfeasors outside the United States. One of the primary goals of the FSIA to bring U.S. rules of foreign sovereign immunity in line with the practices of other nations, and, in particular, to subject foreign states that commit torts in the United States to the same rules of immunity applied against the United States abroad. *See Hearings on H.R. 11,315 Before the Subcomm. on Admin. Law & Gov't Relations of the H. Comm. on the Judiciary*, 94th Cong. 29 (1976) ("1976 Hearing"); 1973 Hearing at 29. Prior to enactment of the FSIA, the United States was often subject to tort suits—most often in Europe—alleging claims that could not be brought against foreign states in U.S. courts. *See* S. Rep. No. 94-1310, at 10–11 (1976). As explained during the hearings on the FSIA, "almost all countries in Western Europe [had come to] follow[] the restrictive theory of sovereign immunity, and permitted . . . suit against the United States in contract and in tort where the necessary contacts with the forum were present." 1976 Hearings at 32 (statement of Bruno Ristau, Chief, Foreign Litigation Section, Civil Division, Dep't of Justice). The non-commercial tort exception, accordingly, can be understood to permit suit against foreign states for torts committed in the United States "to the same extent that the United States [was] subject to suit in most foreign countries." *Id.* at 29.

This same legislative history also reflects an understanding of the European model that Congress sought to mirror. In particular, the legislative record included a copy of the European Convention on State Immunity, which was scheduled to "come into force" roughly a week later. 1976 Hearing at 37. When asked at a hearing whether there was "any inconsistency between that new convention and th[e] bill" that became the FSIA, the Legal Advisor to the State Department answered "no," with the sole qualification that the FSIA went "somewhat further" regarding the execution of judgments against foreign states. *Id.* The relevant provision of the European

Convention on State Immunity provided:

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

Article 11, European Convention on State Immunity, *reprinted in* 1976 Hearings 39 (emphasis added); s*ee also* 1973 Hearing at 32 (referring to proposed convention). The non-commercial tort exception thus sought to parallel the European waiver of sovereign immunity, which required the tortfeasor's physical presence in the jurisdiction of suit.

For the foregoing reasons, the Court holds that Kidane's claim for intrusion upon seclusion is barred by the "entire tort" rule. The political branches may ultimately deem it advisable to permit suits against foreign sovereigns who, without setting foot on American soil, use technology to commit torts against persons located here. But "[i]f the [FSIA] is to be altered, that is a function for the same body that adopted it." *Black*, 564 F.2d at 539 (interpreting FTCA). Absent further action by Congress, any remedy for such alleged misconduct must take place at a diplomatic level.

3. *The Discretionary Function Exception*

Although the Court has already concluded that both of Kidane's claims must be dismissed, given the likelihood that its decision will be appealed and in the interest of judicial efficiency, the Court will also address Ethiopia's final argument why the FSIA bars this action—an argument that is substantial, if ultimately unpersuasive. In particular, Ethiopia argues that the FSIA's discretionary function exception bars Kidane's claim because the alleged conduct "involve[s] an element of choice" and is exactly the kind of "quintessentially political" decision, Dkt. 27-2 at 20, that the exception was designed to shield. The Court disagrees.

The FSIA's discretionary function exception bars a claim that would otherwise fall within the non-commercial tort exception if it is "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). As the D.C. Circuit has explained, the FSIA's discretionary function exception is "analogous" to the FTCA's similar exception. *See MacArthur Area Citizens Ass'n*, 809 F.2d at 922. The D.C. Circuit follows a two-part test in determining whether governmental conduct is shielded as discretionary. Under that test, a court first asks "whether any statute, regulation, or policy specifically prescribes a course of action for an employee to follow." *Banneker Ventures, LLC v. Graham*, 798 F.3d 1119, 1143 (D.C. Cir. 2015). If the employee was following such a policy, his conduct was non-discretionary and subject to liability. *Id.* Second, if the tortfeasor's conduct was not directed by some statute or policy, but instead was the result of discretion, the court asks if "the exercise of discretion [was] grounded in social, economic, or political goals," thus making it "an exercise of governmental judgment and so immune." *Id.*

Ethiopia argues that its conduct falls under the second of these prongs. In its view, because the act of spying on individuals living abroad is a "quintessentially political" one, Dkt. 27-2 at 20, the FSIA's discretionary function exception shields such conduct from suit. Kidane, for his part, argues that a corollary rule to the discretionary function exception makes clear that the alleged conduct falls outside the exception. *See* Dkt. 28 at 31–32. The Supreme Court has long held that when a U.S. official acts outside a grant of discretionary authority, "there will be no shelter from liability because there is no room for choice and the action will be contrary to policy." *See United States v. Gaubert*, 499 U.S. 315, 324 (1991). As the D.C. Circuit has explained this rule, "[a] government official has no discretion to violate the binding laws, regulations, or policies that define the extent of his official powers." *Red Lake Band of*

Chippewa Indians v. United States, 800 F.2d 1178, 1196 (D.C. Cir. 1986). Most courts that have considered the issue have therefore concluded that the FTCA's discretionary function exception does not shield acts *barred* by statute, regulation, or policy—that is, the exception does not apply to illegal acts. *See Banneker Ventures*, 798 F.3d at 1143 (holding that there is "no difference between a *prescription* by policy that leaves no room for choice and a *proscription* that does the same"); *cf. Castro v. United States*, 608 F.3d 266, 271 n.1 (5th Cir. 2010) (en banc) (Stewart, J., dissenting) (collecting cases). Pursuant to this rule, courts have concluded, for instance, that the FTCA's discretionary function exception does not shield government officials who unlawfully open private mail. *See Birnbaum v. United States*, 588 F.2d 319, 329 (2d Cir. 1978); *Cruikshank*, 431 F. Supp. at 1359.

Kidane argues that because Ethiopia's conduct would have violated U.S. criminal law—indeed, would have been a "serious felon[y] under federal law," Dkt. 28 at 31–32—it cannot be protected by the FSIA's discretionary function exception. There is little discussion in the caselaw, however, about how the rule limiting the *FTCA*'s discretionary function exception to the acts of an officer acting within "the extent of his official powers," *see Red Lake*, 800 F.2d at 1196, applies in the context of the *FSIA's* analogous exception. The central inquiry under the FTCA's discretionary function exception is which statute, rule, or policy permitted the relevant U.S. official to exercise "policy judgment"—that is, which rule defines and limits that official's "official powers." *See Dalehite v. United States*, 346 U.S. 15, 36 (1953). But it is less clear how courts should go about identifying such rules when assessing the "discretion" of *foreign* officials, not U.S. officials, to act. Should courts look to U.S. law or to international law? *Cf. Letelier*, 588 F. Supp. at 675 (considering "both national and international law"). Is the law of the foreign

country relevant? *Cf. Liu v. Republic of China*, 892 F.2d 1419, 1431 (9th Cir. 1989) (concluding that it is).

Not surprisingly, Ethiopia argues for the broadest interpretation of the scope of the exception. Citing this Court's decision in *Letelier*, 588 F. Supp. 655, it contends that the "legality of the [foreign state's] activity [under U.S. law] is not the test, but rather whether the activity violates universal norms, such as murder and torture." Dkt. 29 at 16. But *Letelier* did not hold any such thing. The question in that case was whether Chile's assassination of a U.S.-based diplomat was shielded by the FSIA's discretionary function exception. The Court held that it was not, explaining that foreign officials lack "discretion" within the meaning of the FSIA to commit any acts that are "clearly contrary to the precepts of humanity as recognized in both national and international law." 488 F. Supp. at 675. The Court said nothing, however, about whether foreign officials have the "discretion" to commit *less* serious offenses, or, indeed, about whether the ultimate touchstone is "national" or "international" law. *Cf.* Curtis A. Bradley & Jack L. Goldsmith, *Pinochet and International Human Rights Litigation*, 97 Mich. L. Rev. 2129, 2154–55 (1999) (criticizing *Letelier*'s reliance on international law). Yet, other than *Letelier*, Ethiopia offers no authority to support its proposed interpretation of the discretionary function exception. That interpretation, moreover, would render foreign sovereigns immune from dramatically more suits under the FSIA than the United States is under the FTCA, and is thus at odds with Congress's goal of "plac[ing] foreign states in the same position before the United States courts as is the United States itself" when sued under the FTCA. Restatement (Third) of the Foreign Relations Law of the United States § 454 n.3.

The Court also rejects Ethiopia's contention that Ethiopian law should govern the scope of the FSIA's discretionary function exception. As a threshold matter, it is not clear why

Congress would have intended the analysis in an FSIA suit to turn on the meaning of foreign law—an analysis that both the Court and the parties (or at least the plaintiff) are poorly positioned to perform. *Cf. Liu*, 892 F.2d at 1431–32. Even if it were practical for the Court to conduct such an inquiry, moreover, treating foreign law as central to the analysis would run contrary to Congress's intent to place the United States and foreign states on similar footing in U.S. courts. Such an approach would also seem to reward foreign states for adopting rules permitting or encouraging tortious activity in the United States—a purpose that it is difficult to ascribe to Congress. Perhaps most significantly, a focus on foreign authority to act would at least at times require U.S. courts—including state courts, which are also charged with applying the FSIA, *see* 28 U.S.C. § 1605(a)—to "launch[] inquiries into the type of governments that obtain in particular foreign nations," whether particular foreign actions are grounded in law or "are merely [actions] turning upon the whim or caprice of government officials, whether the representation of consuls, ambassadors, and other representatives of foreign nations is credible or made in good faith," and whether particular foreign officials were acting with the implicit or explicit authorization of their superiors. *See Zschernig v. Miller*, 389 U.S. 429, 434 (1968). Such a construction of the Act, in other words, could raise distinct foreign relations concerns going far beyond those already inherent in subjecting foreign states to suit.

Instead, the Court concludes that, in creating a discretionary function exception under the FSIA, Congress did not mean to shield "discretionary" acts by foreign states when those acts involve serious violations of U.S. criminal law. Such a reading of the exception is consistent with the D.C. Circuit's sole opinion touching upon this question, *MacArthur Area Citizens Association v. Republic of Peru*, 809 F.2d 918. In that case, a Washington, D.C. neighborhood association sued Peru for converting a local building, which had been zoned for residential use,

into its chancery. *See id.* at 919. Among other questions, the case turned on whether the discretionary function exception barred the suit. *Id.* at 921–23. In rejecting the plaintiffs' contention that "Peru's acts [we]re criminal and thus [could] not be discretionary," the Court of Appeals acknowledged that "case law buttresses the proposition that a criminal act cannot be discretionary," but concluded that Peru had not been shown to have violated any criminal law. *Id.* at 922 n.4. It added:

> [I]t is hardly clear that, even if a criminal act were shown, it would automatically prevent designation of Peru's acts as discretionary. The cases on which appellant relies involve criminal acts of a rather different character and order. *See, e.g.*, *Letelier*, 488 F. Supp. at 673 (involving "assassination of an individual or individuals, action that is clearly contrary to the precepts of humanity as recognized in both national and international law"). We think it not unduly bold to conclude that violations, if any, of a zoning ordinance do not rise to the level of actions *malum in se*.

Id. Thus, albeit in dicta, *MacArthur Area* suggests that the discretionary function exception does not shield acts by foreign officials that violate federal criminal law, at least if the conduct is *malum in se*.[8] The Restatement provides a similar standard, suggesting that the exception should not apply to "serious criminal act[s]." Restatement (Third) of the Foreign Relations Law of the United States § 454 n.3.

On the present record, the Court can neither conclude that a serious criminal act occurred nor reject the possibility that it did. Various criminal laws, including, most prominently, the

[8] The D.C. Circuit also distinguished cases holding that "[a] government official has no discretion to violate the binding laws, regulations, or policies that define the scope of his official powers," *see Red Lake*, 800 F.2d at 1196, on the ground that "[t]here [wa]s no indication in the record that the" Peruvian officials "were acting *ultra vires*." 809 F.2d at 922 n.3. For the reasons explained above, the Court is unconvinced that the FSIA's discretionary function exception turns on whether the foreign official was acting within the scope of her authority *under foreign law* in committing the alleged tort. In any event, nothing in *MacArthur Area* suggests that authorization under foreign law is sufficient to invoke the discretionary function exception where the conduct at issue constitutes a serious violation of U.S. criminal law.

Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*, make computer trespass a federal crime. *See* S. Rep. No. 104-357, at 11 (1996) (explaining that the CFAA applies to all computer trespasses). Similarly, even though the relevant provision of the Wiretap Act does not apply to foreign states, *see supra* at 7–13, it does apply to the actions of "individuals," and would arguably apply to actions committed by those employed by foreign states. Ethiopia argues that its immunity from suit under the FSIA does not depend on whether it violated these statutes, but does not argue, at this stage, that it did not do so. The Court is thus left without the necessary record upon which to draw a conclusion regarding Ethiopia's conduct (and, accordingly, the applicability of the discretionary function exception). In light of its previous conclusion that the suit should be dismissed under the "entire tort" rule, the Court has no need to direct further briefing on these issues. It has no difficulty, however, rejecting Ethiopia's overbroad interpretations of the scope of the discretionary function exception, and concluding that when a plaintiff alleges underlying conduct that constitutes a serious violation of a U.S. criminal statute, the FSIA's discretionary function exception does not apply.

IV. CONCLUSION

For the foregoing reasons, it is hereby **ORDERED** that Ethiopia's motion to dismiss, Dkt. 27, is **GRANTED.** The Clerk shall enter final judgment.

SO ORDERED.

/s/ Randolph D. Moss
RANDOLPH D. MOSS
United States District Judge

Date: May 24, 2016