ORAL ARGUMENT SCHEDULED FOR FEBRUARY 2, 2017

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 16-7081

JOHN DOE, A.K.A. KIDANE,

Plaintiff-Appellant,

v.

FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA,

Defendant-Appellee.

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

DEFERRED JOINT APPENDIX
VOL. II OF II, PAGES JA 430 TO JA 702

Nathan Cardozo
Cindy Cohn
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Tel. (415) 436-9333

Richard M. Martinez
Samuel L. Walling
Robins Kaplan LLP
800 LaSalle Avenue, Ste. 2800
Minneapolis, MN 55402-2015
Tel. (612) 349-8500

Counsel for Plaintiff-Appellant John Doe

December 14, 2016

Scott A. Gilmore
Guernica 37 Int'l Justice Chambers
Premier House, 3rd Floor
12-13 Hatton Garden
London, U.K EC1N 8AN
Tel. +1 (510) 374-9872

Counsel for Plaintiff-Appellant John Doe

TABLE OF CONTENTS

(Documents from the Record of U.S.D.C. D.C. No. 14-cv-00372-RDM)			
VOLUME I			
ECF No.	**Date**	**Document Description**	**Page**
1	3/5/14	Motion For Leave To Proceed In Pseudonym	JA 001
1-1	3/5/14	Declaration of John Doe (AKA "Kidane") In Support Of Motion For Leave To Proceed In Pseudonym	JA 016
1-2	3/5/14	Declaration of Cindy Cohn In Support Of Motion For Leave To Proceed In Pseudonym	JA 19
2	3/5/14	Order Granting Motion For Leave To Proceed In Pseudonym	JA 429
VOLUME II			
26	7/18/14	First Amended Complaint	JA 430
27	8/4/14	Defendant's Motion To Dismiss Plaintiff's First Amended Complaint	JA 476
28	8/18/14	Plaintiff's Opposition to Defendant's Motion to Dismiss First Amended Complaint	JA 507
29	8/28/14	Defendant's Reply To Plaintiff's Oppostion To Defendant's Motion To Dismiss First Amended Complaint	JA 550
36	7/28/15	Transcript of Motion Hearing Held Before The Honorable Judge Randoph D. Moss on July 14, 2015	JA 575
38	9/25/15	Notice by the United States	JA 664
39	5/24/16	Memorandum Opinion and Order	JA 666
41	6/22/16	Notice of Appeal	JA 702

CERTIFICATE OF FILING AND SERVICE

I, Nathan Cardozo, being duly sworn according to law and being over the age of 18, upon my oath depose and say that:

I am counsel for Appellant and am authorized to electronically file the foregoing DEFERRED JOINT APPENDIX with the Clerk of Court using the CM/ECF System, which will serve via e-mail notice of such filing to all counsel registered as CM/ECF users, including any of the following:

ROBERT PHILLIP CHARROW
LAURA METCOFF KLAUS
THOMAS R. SNIDER
Greenberg Traurig, LLP
2101 L Street NW #1000
Washington, DC 20036

Counsel for Defendant-Appellee
Federal Democratic Republic of Ethiopia

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

Counsel for interested party
United States of America

Dated: December 14, 2016

/s/ *Nathan Cardozo*
Counsel for Appellant

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JOHN DOE, a.k.a. KIDANE, *Plaintiff*, v. FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA, *Defendant*.	Civ. No. 1:14-cv-00372-CKK **FIRST AMENDED COMPLAINT** **JURY TRIAL DEMANDED**

1. Plaintiff John Doe, aka Kidane ("Plaintiff" or "Mr. Kidane") brings this action against the Federal Democratic Republic of Ethiopia ("Defendant" or "Ethiopia") and alleges as follows:

PRELIMINARY STATEMENT

2. This is a straightforward case challenging the wiretapping and invasion of privacy of an American citizen at his home in suburban Maryland. The only significant difference between this an ordinary domestic wiretapping case is that the wiretapping was conducted by the government of Ethiopia.

3. Mr. Kidane is a U.S. citizen who was born in Ethiopia and who has been living in the U.S. for over 22 years.

4. Between late October 2012 and March 2013, Defendant caused Mr. Kidane's personal laptop computer in Maryland to become infected with clandestine computer programs known as FinSpy that, at a minimum, surreptitiously intercepted and contemporaneously

recorded dozens of Mr. Kidane's private Skype[1] Internet phone calls, recorded portions or complete copies of a number of emails sent by Mr. Kidane, and recorded a web search related to the history of sports medicine, conducted by Mr. Kidane's son for his ninth grade history class.

5. As described further below, Plaintiff is informed and believes that his computer became infected because of an email containing a Microsoft Word document attachment, sent by or on behalf of Defendant, that was thereafter forwarded to Plaintiff. The attachment then caused a clandestine client program to be surreptitiously downloaded onto his computer. The downloaded clandestine client program resident on Plaintiff's computer then took what amounts to complete control over the operating system. It began contemporaneously recording some, if not all, of the activities undertaken by users of the computer, including Plaintiff and members of his family, a copy of which was sent to a server in Ethiopia and controlled by Defendant.

6. The programs that accomplished the spying on the Kidane family computer in Maryland are collectively called FinSpy. 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. Finspy is sold exclusively to government agencies and is not available to hackers or the general public.

7. CitizenLab is an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada. CitizenLab focuses on advanced research and development at the intersection of digital media, global security, and human rights.

8. CitizenLab has investigated the use of FinSpy technology by governments to spy on human rights and democracy activists around the world. On March 13, 2013, the CitizenLab

[1] Skype is a voice-over-IP communication service provided by Microsoft. The Skype service allows users to use their computer to communicate with other users by voice (with a microphone), video (with a webcam), and text (via instant messaging). Users may also call numbers on the tranditional telephone network.

released a report on the proliferation of FinSpy. The report included a section describing the Ethiopian Government's use of FinSpy, and included identifying details of a FinSpy Master server in Ethiopia. As described in more detail below, and as demonstrated by the traces of FinSpy left on Mr. Kidane's computer, the FinSpy Master server in Ethiopia disclosed in CitizenLab's report is the same server that controlled the FinSpy target installation on Mr. Kidane's computer.

9. Five days after CitizenLab's report, on or around March 18, 2013, the FinSpy target installation on Mr. Kidane's computer was remotely uninstalled by a command sent by Defendant. However, in an apparent software malfunction, FinSpy's remote uninstall process failed to completely remove all traces of the software from Mr. Kidane's computer.

10. The FinSpy installation on Mr. Kidane's computer was active for at least four and a half months, from early November 2012 until the middle of March 2013. Plaintiff is informed and believes that throughout that period, Defendant Ethiopia caused the FinSpy programs installed on the Kidane family computer in Maryland to create contemporaneous recording of his activities in Maryland, which the FinSpy programs then sent to the FinSpy Master server located in Ethiopia.

11. Mr. Kidane seeks a declaration that Ethiopia's real-time recording of his private Skype communications, and related violations of his right to privacy including the recording of his own and his family's web browsing, was tortious and unlawful.

12. Mr. Kidane additionally seeks statutory damages under the Wiretap Act and damages for Ethiopia's intrusion upon his seclusion.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction and personal jurisdiction over the Federal Democratic Republic of Ethiopia pursuant to 28 U.S.C. § 1330 and the Foreign Sovereign Immunities Act (the "FSIA"), 28 U.S.C. §§ 1602, *et seq*., for the multiple tortious injuries occurring within the territory of the United States as alleged in this complaint. Process has been served on the Federal Democratic Republic of Ethiopia pursuant to 28 U.S.C. § 1608(a) (*see* ECF No. 18).

14. Specifically, this Court has subject matter jurisdiction over the Federal Democratic Republic of Ethiopia under 28 U.S.C. §§ 1603(a), 1605(a)(5), and 1606 as Defendant is a foreign state, which is not immune from any suit seeking 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 while acting within the scope of his office or employment"; and where the claim is not based on the lawful exercise of a "discretionary function," and does not arise out of "malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights."

15. As alleged in this complaint, Defendant or Defendant's officials or employees caused personal injury to Plaintiff, a U.S. citizen and resident of the United States, entirely at Plaintiff's residence in Silver Spring, Maryland, in the United States, through the tortious invasion of Plaintiff's privacy and the unlawful interception of Plaintiff's communications, wholly within the territory of the United States, in violation of the Wiretap Act, 18 U.S.C. §§ 2511, 2520.

16. Alternatively, this Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, which confers upon district courts "original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States."

17. Moreover, this Court possesses supplemental jurisdiction over Plaintiff's additional claims pursuant to 28 U.S.C. § 1367(a).

18. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(f)(4) because Defendant is a foreign state.

PARTIES

19. Plaintiff John Doe, also known as Kidane, is an Ethiopian-born citizen of the United States, who currently and at all times relevant to this Complaint resided in Silver Spring, Maryland.

20. Plaintiff uses the name Kidane within the Ethiopian Diaspora in order to protect his family both in the United States and in Ethiopia. Plaintiff's use of the name Kidane was described in detail in Plaintiff's Motion for Leave to Proceed Anonymously, filed concurrently with the original Complaint in this action, and granted by the Court on March 5, 2014 (ECF No. 2). Plaintiff fears that his work within the Ethiopian Diaspora puts his life, and the lives of his family, at substantial risk. *See* Declaration of Kidane (ECF No. 1-1).

21. Defendant the Federal Democratic Republic of Ethiopia is a sovereign state located in East Africa.

FACTUAL ALLEGATIONS

SUPPRESSION OF DISSENT BY THE ETHIOPIAN GOVERNMENT

22. According to the State Department's Report on Human Rights Practices for 2012 in Ethiopia: "The most significant human rights problems [in Ethiopia] include[] restrictions on

freedom of expression and association through politically motivated trials and convictions of opposition political figures, activists, journalists, and bloggers, as well as increased restrictions on print media."[2]

23. In a May 16, 2012 press release, Amnesty International reports that: "The Ethiopian People's Revolutionary Democratic Front (EPDRF) has ruled for more than two decades. [Ethiopian Prime Minister Meles] Zenawi's government has systematically attempted to crush dissent in the country by jailing opposition members and journalists, firing on unarmed protesters, and using state resources to undermine political opposition."[3]

24. The Ethiopian government seeks to undermine political opposition abroad as well as at home. For example, according to the website for the United Nations High Commissioner for Refugees, summarizing an October 11, 2012 report by the Norwegian Broadcasting Corporation: "The Norwegian Broadcasting Corporation (NRK) reports that refugee espionage in Norway is widespread. The espionage often seeks information about refugees in opposition to the regime in their country of origin. This is confirmed by the Norwegian Police Security Service (PST), which adds that several countries carry out refugee espionage in Norway, especially countries in conflict. Rune Berglund Steen, from [the] Antiracism Centre in Oslo, says that: Based on the information I have collected since 2004/2005, it appears that Ethiopian refugee espionage is both systematic and comprehensive. It is shamelessly extensive. He claims that

[2] United States Department of State, Country Reports on Human Rights Practices for 2012, http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2012&dlid=204120 (last visited December 20, 2013).
[3] Amnesty International, http://www.amnestyusa.org/news/press-releases/amnesty-international-urges-president-obama-to-speak-up-about-repression-human-rights-abuses-in-ethi (last visited December 20, 2013).

this has been going on for a long period and that the espionage has not been associated with legal consequences in Norway."[4]

25. One way in which the Ethiopian government monitors political dissidents at home and abroad is through the use of electronic surveillance. According to Freedom House's "Freedom on the Net 2013" report on Ethiopia: "In 2012, [Ethiopian] repression against bloggers and ICT users increased, with several arrests and at least one prosecution reported. The Telecom Fraud Offences law enacted in September 2012 toughened the ban on advanced Internet applications and established criminal liability for certain types of content communicated electronically. Furthermore, monitoring of online activity and interception of digital communications intensified, with the deployment of FinFisher surveillance technology against users confirmed in early 2013." [5]

FINSPY BACKGROUND

26. Exhibit B is a March 13, 2013 report by CitizenLab titled "You Only Click Twice: FinFisher's Global Proliferation." (FinSpy is a part of Gamma's FinFisher line of products.) The report describes the results of a comprehensive global scan of computers on the Internet to identify the command and control servers of FinFisher's surveillance software. It also details the discovery of a campaign using FinFisher in Ethiopia used to target individuals linked to an opposition group.

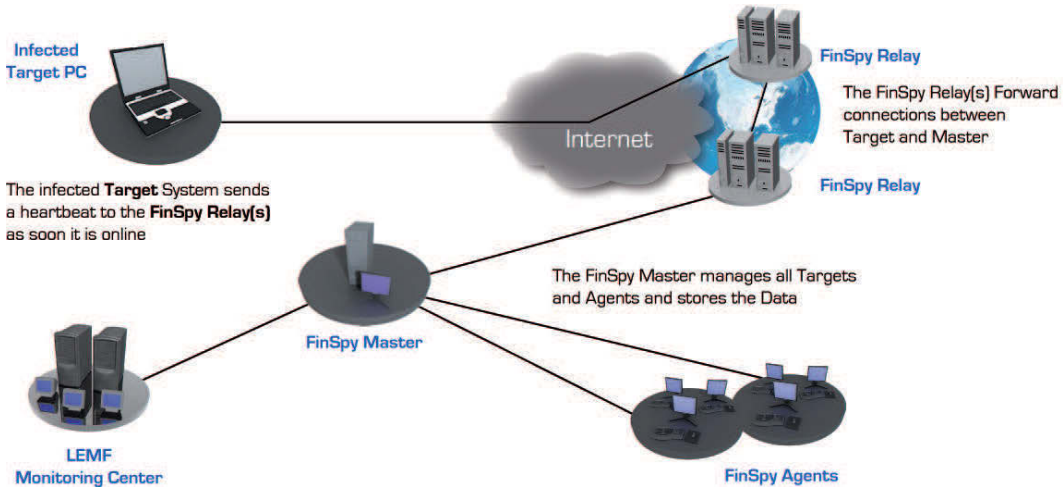
27. FinSpy is part of the FinFisher line of "IT Intrusion" products developed and marketed by the Gamma Group of Companies. The Gamma Group produces FinSpy spyware

[4] UNHCR, http://www.unhcr.se/no/media/baltic-and-nordic-headlines/2012/october/12-16-october-2012.html (last visited December 20, 2013).
[5] Freedom House, http://www.freedomhouse.org/report/freedom-net/2013/Ethiopia (last visited December 20, 2013).

for Windows, Macintosh, and Linux computers, as well as iPhone, Android, Nokia/Symbian, Windows Phone, and Blackberry mobile devices.

28. FinSpy consists of a suite of surveillance software marketed by Gamma International, Ltd, a United Kingdom-based company and/or FinFisher GmbH, a German company (collectively "Gamma"). The software suite includes the target installation of a clandestine client program, one or more FinSpy Relays, and a FinSpy Master server (collectively "FinSpy"). Attached hereto as Exhibit A is a FinSpy sales brochure produced by Gamma.

29. The following diagram illustrates how the FinSpy software operates.



30. Gamma specifically asserts that "FinFisher solutions are sold to governmental agencies only."[6] Plaintiff is informed and believes that FinSpy is therefore unavailable to the general public.

31. According to Gamma's promotional materials, the system consists of client software designed to be covertly installed on a targeted device ("spyware") as well as infrastructure run by the government operator of the system to collect the data gathered by the

[6] FinFisher, http://www.finfisher.com/FinFisher/products_and_services.html (last visited January 9, 2014).

spyware and facilitate monitoring. Devices on which the spyware is installed are referred to as "infected devices."

32. Gamma performs testing of FinSpy against the 40 most popular computer programs for detecting viruses and spyware – known as anti-virus programs (*see* Exhibit A). Gamma routinely modifies FinSpy to prevent detection by anti-virus programs, and releases such updates for FinSpy to their customers.

33. Gamma employs sophisticated techniques to prevent detection and thwart analysis of how its FinSpy spyware works, such that FinSpy is designed specifically to subvert analysis tools used by security researchers.

34. FinSpy is written in a special programming language designed by Gamma. The language is translated into one that the computer can understand and execute as the spyware is run. Performing some kinds of analysis of the spyware require understanding and decoding this language. The spyware can be made to appear to have very different characteristics by making small changes to the language.

35. The infrastructure for collecting data gathered from infected devices consists of software and hardware components known as a FinSpy Master, and one or more FinSpy Relays. The FinSpy Master's job is to facilitate data gathering and monitoring of the devices. The FinSpy Master sends commands to infected devices and receives gathered information.

36. The FinSpy system contains a number of modules (sets of optional computer program components that enable various features) that the government operator may install on infected devices to facilitate different types of monitoring and the acquisition of different types of data from infected devices. For example, FinSpy contains a module for extracting saved

passwords from more than 20 different web browsers, e-mail programs, and chat programs, and capturing these passwords as the user types them in.

37. FinSpy also contains a module for the contemperaneous recording of Internet telephone calls, text messages, and file transfers transmitted through the Skype application, a module for covertly recording audio from a computer's microphone even when no Skype calls are taking place, a module for recording every keystroke on the computer, and a module for recording a picture of the contents displayed on a computer's screen.

38. The FinSpy Skype module uses functionality built into Skype for contemporaneously recording calls. Specifically, the Skype software allows other software to direct Skype to perform certain functions, such as recording call audio while the call is being made. When the FinSpy Skype module on an infected computer records Skype call audio, it does so contemporaneous to the call and without the user's knowledge or consent.

39. The FinSpy spyware is installed by way of a software executable (an executable is any computer file that contains commands for the computer to run, *e.g.*, an application). A government agent can manually install a FinSpy executable on any computer he has physical or remote access to. If the government agent wishes to infect a computer that he does not have physical or remote access to, the agent may send the target a file that contains a FinSpy executable (*e.g.*, via e-mail) and attempt to convince the target to open it on the target's own computer.

40. The types of files that a FinSpy operator may send include a FinSpy executable disguised as an image, or a FinSpy executable embedded in a Microsoft Word document. The government agent may attempt to convince the target to open the file by claiming that the file is

of interest to the target. When the target opens the file, he is presented with a legitimate image or Word Document, depending on the type of file.

41. In the case of the image, the target is tricked into opening the executable and is thus infected. The executable deletes itself, and replaces itself with the benign image displayed to the target. The target is therefore unaware that his computer has been infected.

42. In the case of the Microsoft Word document, the document contains a "macro" – a Microsoft Word feature designed to enable automation – that attempts to run the embedded FinSpy executable when the document is loaded. The Word document does not replace itself with a benign copy after the user is infected. Thus, opening the document again on another computer will also infect that computer. When the executable is run, it creates a directory ("FinSpy directory") on the target computer's disk that it uses to store files, including Skype audio calls, as FinSpy interepts them.

43. Each FinSpy executable contains a configuration file that dictates particular parameters of the operation of that instance of the spyware. One of the parameters specified by the configuration file is a list of one or more Internet addresses or Internet domain names, representing FinSpy Masters with which the spyware should communicate. That perameter is hard-coded into the executable and uniquely identifies the FinSpy Master responsible for that particular infection.

44. Gamma sells FinSpy licenses to governments that only allow a certain number of infected devices to be concurrently monitored (*see* Exhibit A). This number is dictated by the license agreement between Gamma and the government operator of FinSpy.

45. When a device is infected with FinSpy, it contacts the FinSpy Master, through the FinSpy Relay listed in its configuration file. If the number of infected devices is less than the

maximum number that the government operator has purchased licenses for monitoring, then the infection becomes active. If the number of devices being concurrently monitored is equal to the maximum number that are permitted to be concurrently monitored, the infection remains dormant, but periodically contacts the FinSpy Master server to check whether the number of infected devices has dropped below this threshold. If this happens, or if the government operator purchases more licenses from Gamma, then the infection becomes active.

46. When an infection becomes active, it contacts the FinSpy Relay to download modules, and begins capturing and sending information back to the FinSpy Master. In turn, the FinSpy Relay can send commands to an infected device.

47. On information and belief, these commands include the ability to remotely deactivate the spyware on an infected device (*see* Exhibit A). Commands also enable the government operator to specify a new Internet address or domain name as a FinSpy Relay, to install modules, to run custom programs on an infected device, to browse information stored on the device, and to enable or disable features such as live audio recording from the device's microphone.

48. Most of the FinSpy modules, including the module for recording Skype calls, behave in the following manner: The FinSpy module simultaneously records the audio data to the infected computer's disk as as the call proceeds, before then transmitting it to the FinSpy Master. In some cases, such as the case of the FinSpy Skype module, the module first contemporaneously intercepts and copies the data, unencrypted, to files on the infected computer's temporary folder on its hard disk. The module then encrypts the information, and writes it to an encrypted file in the FinSpy directory on the hard disk using a specialized naming

convention that identies files containing captured data. Thus, FinSpy makes a simultaneous recording of a target's Skype call, on his or her own computer.

49. Under the FinSpy naming convention, files containing incoming audio recorded during Skype calls begins with "snd" and ends in between one and four hexadecimal digits. A hexadecimal digital is a base-16 number, in which 0–9 represent values zero to nine, and A, B, C, D, E, F (or alternatively a–f) represent values ten to fifteen.

50. Under ideal conditions, the temporary file is deleted after the encrypted file is successfully written. However, security researchers have observed that FinSpy fails to delete temporary files in some cases.

51. Periodically, FinSpy transmits to the FinSpy Master all files matching the naming convention for files containing captured data. FinSpy deletes these files after it successfully transmits them to the FinSpy Master.

52. In the normal course of operation, whenever any program writes a file to a computer's disk, the computer automatically records the date and time that the file was written, and stores at least the latest such date (along with the file) on disk – previous dates are sometimes stored as well.

53. Security researchers have observed that in some cases, FinSpy interferes with this process, and backdates some files it writes by exactly one year. Plaintiff is informed and believes that such backdating is a feature of FinSpy that is designed to, in some cases, make the infection slightly more difficult to detect.

54. When a device is infected with FinSpy, the infection may persist on the computer – *i.e.*, when the computer is restarted, it will still be infected with FinSpy. One of the

ways this is achieved is by modifying the computer's boot process.[7] The spyware places itself on normally-unused parts of the disk that are not typically accessible to the computer's operating system. This is known as unpartitioned space. The computer's boot process is modified so that FinSpy is loaded before the computer's operating system. As the computer's operating system loads, FinSpy infects the operating system. Thus, even if FinSpy is removed from the areas of disk normally visible and accessible to the operating system, the boot process can still reinfect the computer when it is restarted.

THE SPECIFIC INFECTION OF PLAINTIFF'S COMPUTER BY FINSPY

55. On or around March 2013, the disk in Plaintiff's computer contained two Microsoft Word documents GKO2.doc and GKO2 (1).doc, which, in turn, contained FinSpy executables designed to infect computers running Microsoft Windows.

56. When the files are opened on a computer, they display several paragraphs of Amharic[8] text in Microsoft Word (*see* Exhibit C, email forwarded to Plaintiff, including original Word document text and accompanying English translation). At the same time, a macro in the document attempts to infect the user's computer with FinSpy. The date on these files were October 31, 2012 at 09:25:17 and October 31, 2012 at 09:25:46 respectively. The Amharic text found on Plaintiff's computer contains a not-so-veiled threat against the family of one of Plaintiff's acquaintences and implies that Defendant, the Government of Ethiopia, is behind both the threat and the email. On information and belief, Defendant created the document whose text appears at Exhibit C, and intentionally infected the document with FinSpy.

[7] A computer's boot process is the series of steps a computer takes automatically when powered on to load the operating system, *e.g.*, Micorosft Windows.
[8] Amharic is the official working language of the Federal Democratic Republic of Ethiopia.

57. On or around March 2013, there was a copy of FinSpy in GKO.doc and GKO (1).doc on Plaintiff's computer.

58. This copy of FinSpy contained a configuration file, hard-coded with an Internet Protocol ("IP")[9] address, 213.55.99.74, for a single FinSpy Relay.

59. The 213.55.99.74 IP address is in a block of addresses registered to Defendant Ethiopia's state-owned telecommunications company[10] – Ethio Telecom.

60. On information and belief, this relay is located inside Ethiopia, and its operator is the Defendant in this action.

61. Online security researchers have conducted several scans of various ranges of Internet address numbers. As a result of one such scan, the existence of the Ethiopian FinSpy Relay located at 213.55.99.74 was first disclosed on August 8, 2012 in a research blog post appearing on the website of Rapid7, a security firm.[11]

62. CitizenLab conducted subsequent scans that determined that the 213.55.99.74 address was a FinSpy Relay located in Ethiopia. These results were publicized on August 29, 2012, and March 13, 2013 (*see* Exhibit B). In both cases, the Relay was still operational at the time of publication.

63. The March 13, 2013 CitizenLab publication also reported on the discovery of a FinSpy infection executable disguised as an image of Ethiopian opposition leaders, which

[9] An IP address is a numeric value used to identify the network location of a computer or set of computers on the Internet. Every computer on the Internet needs to have an IP address in order to communicate with other computers on the Internet.

[10] IP addresses are allocated in blocks of consecutive addresses out of a worldwide pool of around four billion possible addresses though geographically based non-profit organizations known as regional Internet registries.

[11] Rapid7, Information Security: Analysis of the FinFisher Lawful Interception Malware, https://community.rapid7.com/community/infosec/blog/2012/08/08/finfisher (last visited November 13, 2013).

contained a configuration file containing the address of the same Ethiopian relay (*see* Exhibit B). On information and belief, the FinSpy infection executable discovered by CitizenLab was created by Defendant for the purpose of infecting the computers of those who sympathize with the political opponents of Defendant.

64. The hard disk in Plaintiff's computer contains a number of temporary files whose names are consistent with the temporary file naming convention used by FinSpy.

65. The FinSpy software recorded these files on Plaintiff's computer in Maryland, saving them simultaneously on that compuer without Plaintiff's knowledge or consent. Due to the operation of FinSpy, 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.

66. Specifically, the hard disk in Plaintiff's computer contains 244 files whose name begins with "snd" and ends in between one and four hexadecimal digits. FinSpy uses this naming convention for incoming audio recorded during Skype calls.

67. The hard disk contains 247 files whose name begins with "mic" and ends in one to four hexadecimal digits. FinSpy uses this naming convention for audio recorded from the microphone during Skype calls (outgoing audio).

68. FinSpy's Skype module operates as follows: after recording the two audio streams – incoming and outgoing – from a Skype call separately, these two streams are combined into a single file: the incoming audio is placed in the right stereo channel, and the outgoing audio is placed in the left stereo channel. Then this file is compressed to reduce size. FinSpy stores the result of this process in a temporary file whose name begins with "ogg" and ends in one to four hexadecimal digits.

69. The disk in Plaintiff's computer contains 83 such "ogg" files consistent with FinSpy's naming convention. These files contain portions or complete copies of Plaintiff's private and highly confidential Skype conversations.

70. Collectively, the traces of the FinSpy infection found on Plaintiff's computer are referred to as the "FinSpy trace files."

71. Under ideal conditions, FinSpy deletes these temporary files when it is done with them. The presence of the "snd," "mic," and "ogg" files is consistent with Skype calls that were recorded by FinSpy, and in the normal course of FinSpy's operation, would have been transmitted to the FinSpy Master by way of a FinSpy Relay (*see* Exhibit A for an illustration of the operation of a FinSpy Relay).

72. The earliest date observed on any of these FinSpy trace files was December 7, 2011 at 09:35:48.[12] This file appears have been backdated by exactly one year, consistent with FinSpy's observed behavior. The latest date observed on any of these FinSpy trace files was March 17, 2013 at 17:30:35.

73. FinSpy also stores temporary files whose names begin with "del" and end in one to four hexadecimal digits. The disk contains 1597 such files. The latest date observed on any of these files was March 18, 2013 at 08:58:24.

74. The disk in Plaintiff's computer also contains a folder ProtectedSvc that was used by FinSpy to store various components of FinSpy, including its code, configuration file, and encrypted files containing gathered data before they are sent to the server. Some of the non-Skype files recorded by FinSpy on Plaintiff's computer include recordings of his, and his family's, web search histories, including a record of Mr. Kidane's son's search related to sports

[12] All times are Eastern time and written in 24-hour format.

medicine. Several of the other files appear to be FinSpy records of other of Mr. Kidane's computer activity.

75. The date on the folder was October 31, 2011 at 09:26:39. On information and belief, the time on the ProtectedSvc folder was backdated by FinSpy by exactly one year. Therefore, Plaintiff is informed and believes that October 31, 2012 was the date Defendant Ethiopia infected his computer.

76. The ProtectedSvc folder on Plaintiff's computer also contains FinSpy code, a configuration file, and several encrypted files containing gathered data that were apparently not sent to the server. The most recent date associated with the folder is March 18, 2013 at 08:58:27. This is also the most recent date associated with any file on Plaintiff's disk that is consistent with a file written by or belonging to FinSpy. This is Plaintiff's best estimate for the last date of activity of FinSpy on Plaintiff's computer.

77. In summary, Plaintiff's computer was infected with FinSpy on October 31, 2012 at 09:26:39. The earliest date associated with files containing modules downloaded from the server is November 12, 2011 at 08:23:14. This is consistent with FinSpy's technique of backdating files by exactly one year, so the best available estimate for when the infection became active is November 12, 2012 at 08:23:14. During the time that the infection was active, FinSpy operated on Plaintiff's computer in Maryland to contemporaneously intercept his private Skype calls as well as private details of his family's computer usage, and record them to the computer's hard disk without Plaintiff's knowledge or consent. The infection appears to have been removed on March 18, 2013 at 08:58:27, just five days after CitizenLab's publication of its report disclosing Defendant Ethiopia's use of FinSpy and the technical details of the FinSpy Relay in use in Ethiopia. On information and belief, FinSpy is sold only to governments and government

agencies, and the instance of FinSpy that was present on Plaintiff's computer was hard-coded to report back to a server controlled by Defendant.

SUMMARY OF ALLEGATIONS

78. Gamma expressly represents that it only sells the FinSpy product to law enforcement and intelligence agencies.

79. Defendant Ethiopia controls all Ethiopian law enforcement and intelligence agencies.

80. On information and belief, Gamma sold the FinSpy software suite to Defendant Ethiopia.

81. Defendant Ethiopia intentionally distributed a Microsoft Word document infected with FinSpy.

82. Plaintiff's computer in Maryland was infected by a FinSpy executable created by Defendant on or around October 31, 2012 at 09:26:39 by that Microsoft Word file.

83. The FinSpy installation on Plaintiff's computer in Maryland directly resulted from the Microsoft Word document file intentionally created and intentionally infected with FinSpy by Ethiopia.

84. The FinSpy installation on Plaintiff's computer in Maryland took instructions from a FinSpy Relay controlled by Defendant Ethiopia.

85. On information and belief, the FinSpy Relay and FinSpy Master servers with which Plaintiff's computer in Maryland was controlled are located inside Ethiopia and controlled by Defendant Ethiopia.

86. The FinSpy installation on Plaintiff's computer in Maryland downloaded modules from this FinSpy Master server onto Platinff's computer on or around November 12, 2012 at 08:23:14.

87. On information and belief, the FinSpy software on Plaintiff's computer in Maryland used the downloaded modules to automatically intercept Plaintiff's private commmunications, resulting in a contemporaneous interception of Plaintiff's communications on his computer in Maryland.

88. Defendant Ethiopia attempted to remove the FinSpy software infection from Plaintiff's computer in Maryland on or around March 18, 2013 at 08:58:27, just five days after CitizenLab published technical details describing the FinSpy Relay operated by Defendant—the same server that was controlling Plaintiff's computer.

89. On information and belief, the FinSpy installation on Plaintiff's computer in Maryland was controled by Defendant Ethiopia at all times between October 2012 and March 2013.

90. On information and belief, Defendant Ethiopia did not obtain a warrant, work with the United States Department of State, or obtain any legal process to lawfully undertake a wiretapping of Plaintiff at his home in Maryland.

91. The knowledge that Defendant Ethiopia had access to Plaintiff's most sensitive private communications, including those involving this work with the Ethiopian Diaspora, puts Plaintiff at substantial unease and has caused him significant emotional distress. Defendant's actions have caused Plaintiff to fear for his safety, as well as that of his friends, family, and contacts.

FIRST CAUSE OF ACTION

Violation of the Wiretap Act, 18 U.S.C. § 2511

92. Plaintiff repeats and incorporates herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

93. The Wiretap Act prohibits the willful interception of any wire, oral, or electronic communication.

94. A private right of action is created by 18 U.S.C. § 2520 and is available to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used."

95. Defendant intentionally and willfully intercepted Plaintiff's private wire, oral, or electronic communications, using a software device on Plaintiff's computer at his home in Silver Spring, Maryland.

96. Among other data intercepted by Defendant, Plaintiff's private Skype calls were wire, oral, or electronic communications within the meaning of the Wiretap Act.

97. Defendant Ethiopia's contemporaneous acquisition of Plaintiff's private Skype phone calls, by the use of the FinSpy software present on Plaintiff's computer in the United States, is an interception within the meaning of the Wiretap Act because it is an acquisition of the contents of his communication by use of any electronic, mechanical, or other device.

98. Plaintiff had a reasonable expectation that his wire, oral, or electronic communications would remain private.

99. Plaintiff is a person whose wire, oral, or electronic communication were intercepted within the meaning of 18 U.S.C. § 2520.

100. Section 2520 provides for equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each violation of the Wiretap Act, and reasonable attorneys' fees as a result of the above-described violations.

SECOND CAUSE OF ACTION

Intrusion Upon Seclusion

101. Plaintiff repeats and incorporates herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

102. Defendant intentionally intruded upon and invaded the solitude and seclusion of Plaintiff.

103. Defendant intruded upon and invaded Plaintiff's private affairs and concerns by using a software device on Plaintiff's computer at his home in Silver Spring, Maryland, to record and monitor Plaintiff's and his family's computer private activities at their home in Maryland, and to transmit said recordings to servers it controlled in Ethiopia.

104. Plaintiff's private affairs and concerns, including his wire, oral, or electronic communications intercepted by Defendant, are not a matter of public concern.

105. The aforementioned intrusion upon seclusion was highly offensive to an ordinary, reasonable person.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court:

1. Declare that Defendant's actions as described above violated the Wiretap Act, and constituted an intrusion upon seclusion;

2. Award to Plaintiff damages, including statutory damages where available, for injury sustained by him as a result of Defendant's wrongdoing, in an amount to be proven at trial, including pre-judgment interest thereon;

3. Award to Plaintiff reasonable attorneys' fees and other costs and expenses of suit to the extent permitted by law; and

4. Grant Plaintiff such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff hereby requests a trial by jury for all issues so triable.

Dated: July 17, 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

Exhibit A

Exhibit A

FINSPY

FinSpy is a field-proven Remote Monitoring Solution that enables Governments to face the current challenges of **monitoring Mobile and Security-Aware Targets** that regularly **change location**, use **encrypted and anonymous communication** channels and **reside in foreign countries**.

Traditional Lawful Interception solutions face new **challenges** that can only be solved using active systems like FinSpy:
· Data not transmitted over any network
· Encrypted Communications
· Targets in foreign countries

FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

QUICK INFORMATION	
Usage:	· **Strategic Operations** · **Tactical Operations**
Capabilities:	· **Remote Computer Monitoring** · **Monitoring of Encrypted Communications**
Content:	· **Hardware/Software**

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Computer – Example Features:

· Bypassing of 40 regularly tested Antivirus Systems
· **Covert Communication** with Headquarters
· Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
· Recording of **common communication** like Email, Chats and Voice-over-IP
· **Live Surveillance** through Webcam and Microphone
· **Country Tracing** of Target
· **Silent extracting of Files** from Hard-Disk
· **Process-based Key-logger** for faster analysis
· **Live Remote Forensics** on Target System
· **Advanced Filters** to record only important information
· Supports most common Operating Systems (**Windows, Mac OSX** and **Linux**)

Headquarters – Example Features:

· Evidence Protection (Valid Evidence according to **European Standards**)
· **User-Management** according to Security Clearances
· Security Data Encryption and Communication using **RSA 2048 and AES 256**
· Hidden from Public through **Anonymizing Proxies**
· Can be **fully integrated** with Law Enforcement Monitoring Functionality (LEMF)

For a full feature list please refer to the Product Specifications.

Product Components

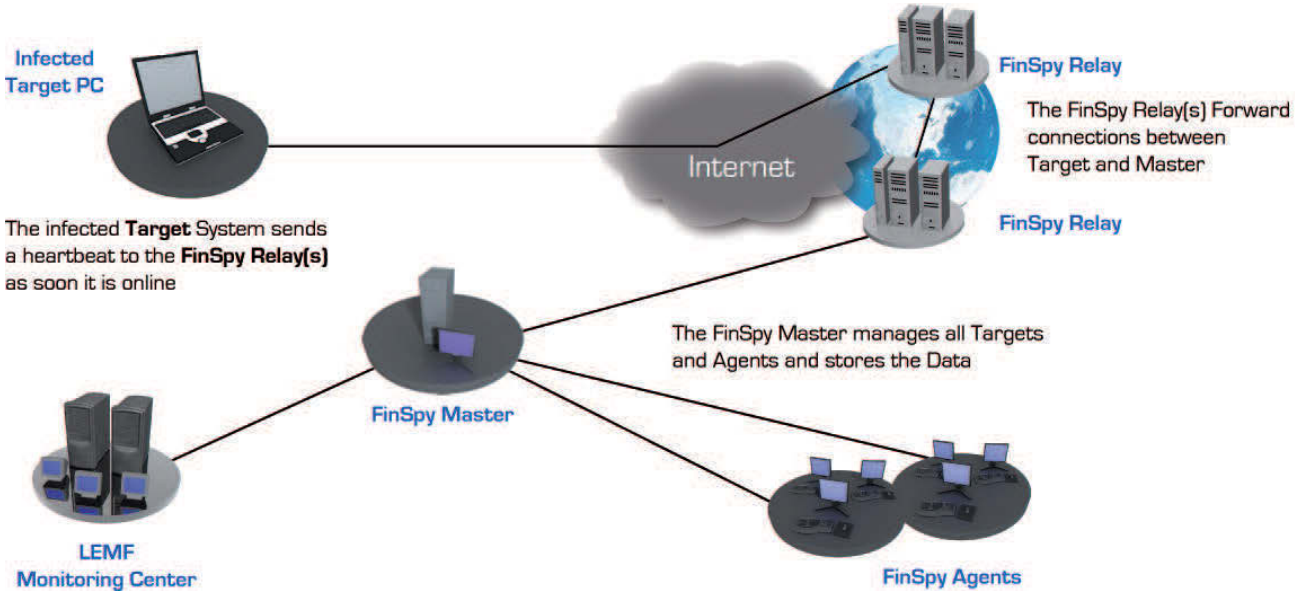
FinSpy Master and Proxy

- Full Control of Target Systems
- Evidence Protection for Data and Activity Logs
- Secure Storage
- Security-Clearance based User- and Target Management

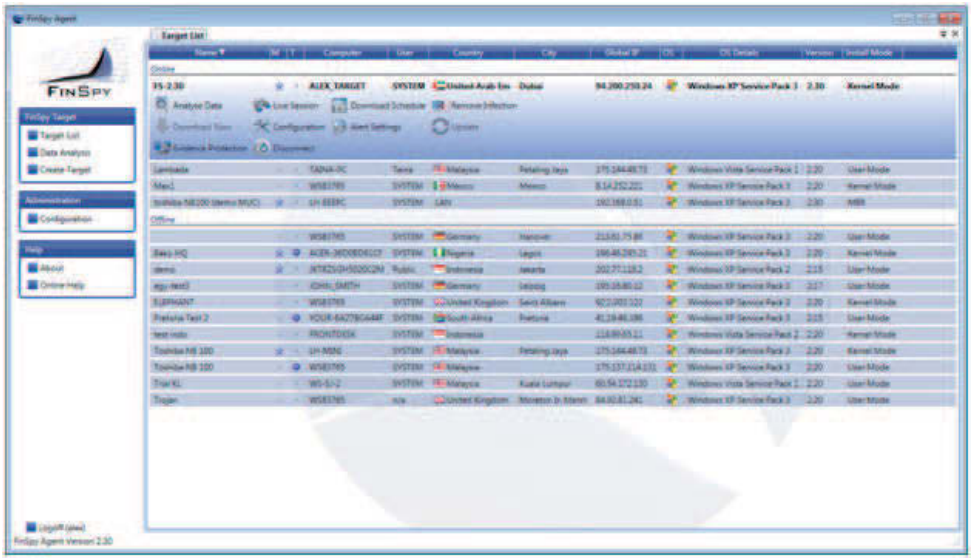
FinSpy Agent

- Graphical User Interface for Live Sessions, Configuration and Data Analysis of Targets

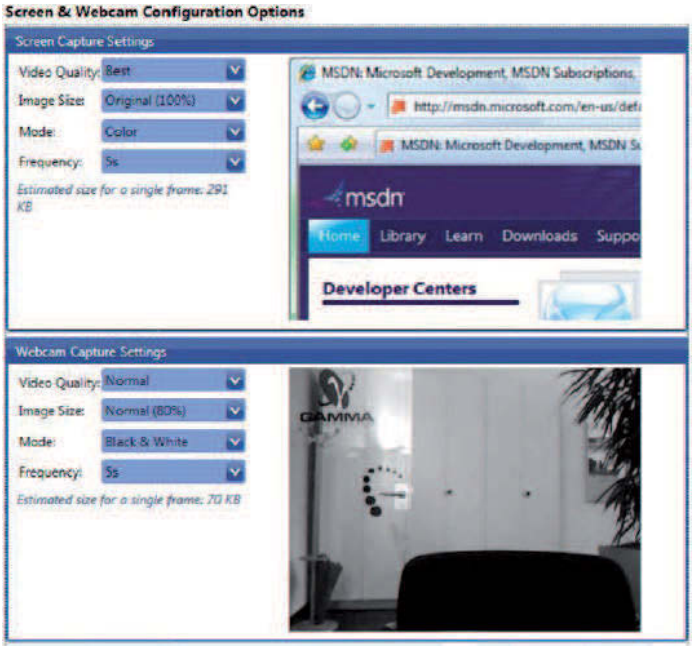
Access Target Computer Systems around the World



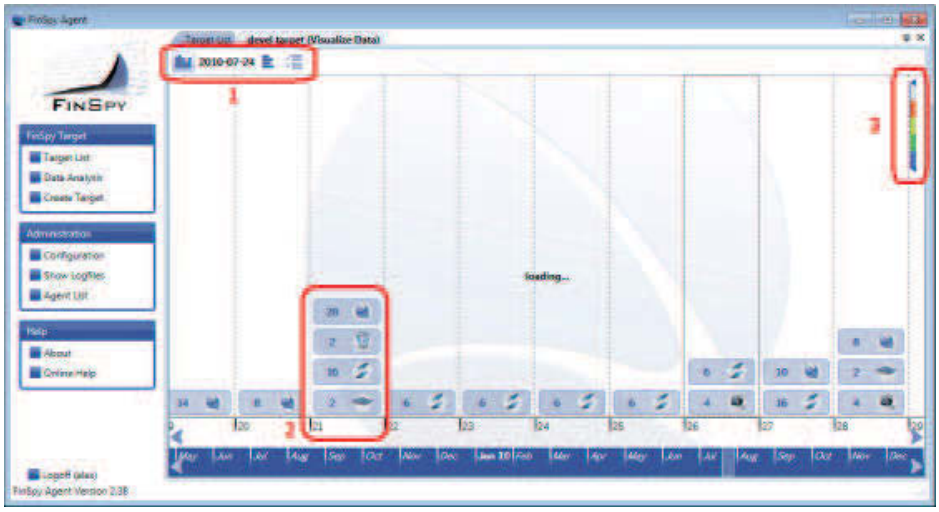
Easy to Use User Interface



Live and Offline Target Configuration



Full Intelligence on Target System



1. Multiple Data Views
2. Structured Data Analysis
3. Importance Levels for all recorded Files

FINSPY LICENSES

Outline

The FinSpy solution contains 3 types of product licenses:

A. Update License

The Update License controls whether **FinSpy** is able to retrieve new updates from the Gamma Update server. It is combined with the **FinFisher™ After Sales Support** module.After expiry, the **FinSpy** system will still be **fully functional** but no longer able to retrieve the newest versions and bug-fixes from the FinSpy Update server.

B. Agent License

The Agent License controls how many **FinSpy Agents** can login to the **FinSpy Master** in parallel.

Example:

- **5 Agent Licenses** are purchased.
- **FinSpy Agent** licenses can be installed on an unlimited number of systems, however
- Only 5 **FinSpy Agent** systems can login to the **FinSpy Master** and work with the **data at the same time**

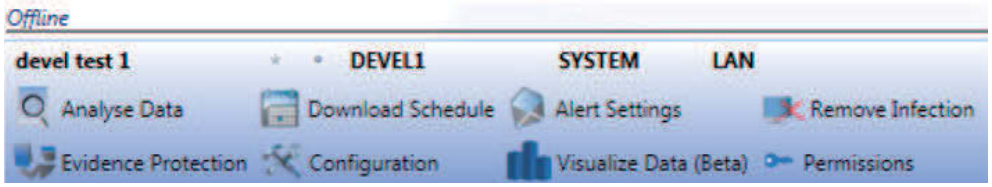
C. Target License

The Target License controls how many **FinSpy Targets** can be **active** in parallel.

Active refers to **activated FinSpy Target** installations no matter whether the Target System is online or offline.

When **FinSpy Target** is deployed on a Target System and no Target Licenses are available, the **FinSpy Target** gets temporary deactivated and no recording and live access will be possible. As soon as a new License is available (e.g. by upgrading the existing License or de-infecting one of the active **FinSpy Targets**), the Target will be assigned the free license and it will be activated and begin recording and providing live access.

Screenshot active Target with License



Screenshot inactive Target without License

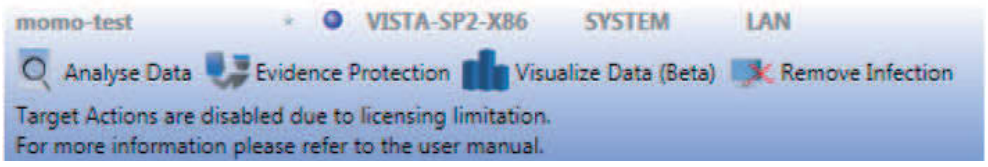


Exhibit B

Exhibit B

UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS
Join the Global Conversation

The Citizen Lab

Research Brief
Number 15 – March 2013

You Only Click Twice:

FinFisher's Global Proliferation

Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton.

This post describes the results of a comprehensive global Internet scan for the command and control servers of FinFisher's surveillance software. It also details the discovery of a campaign using FinFisher in Ethiopia used to target individuals linked to an opposition group. Additionally, it provides examination of a FinSpy Mobile sample found in the wild, which appears to have been used in Vietnam.

1. SUMMARY OF KEY FINDINGS

- We have found command and control servers for FinSpy backdoors, part of Gamma International's FinFisher "remote monitoring solution," in a total of 25 countries: Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam.
- A FinSpy campaign in Ethiopia uses pictures of Ginbot 7, an Ethiopian opposition group, as bait to infect users. This continues the theme of FinSpy deployments with strong indications of politically-motivated targeting.
- There is strong evidence of a Vietnamese FinSpy Mobile Campaign. We found an Android FinSpy Mobile sample in the wild with a command & control server in Vietnam that also exfiltrates text messages to a local phone number.
- These findings call into question claims by Gamma International that previously reported servers were *not* part of their product line, and that previously discovered copies of their software were either stolen or demo copies.

2. BACKGROUND AND INTRODUCTION

FinFisher is a line of remote intrusion and surveillance software developed by Munich-based Gamma International GmbH. FinFisher products are marketed and sold exclusively to law enforcement and intelligence agencies by the UK-based Gamma Group.[1] Although touted as a "lawful interception" suite for monitoring criminals, FinFisher has gained notoriety because it has been used in targeted attacks against human rights campaigners and opposition activists in countries with questionable human rights records.[2]

In late July 2012, we published the results of an investigation into a suspicious e-mail campaign targeting Bahraini activists.[3] We analyzed the attachments and discovered that they contained the FinSpy spyware, FinFisher's remote monitoring product. FinSpy captures information from an infected computer, such as passwords and Skype calls, and sends the information to a FinSpy command & control (C2) server. The attachments we analyzed sent data to a command & control server inside Bahrain.

This discovery motivated researchers to search for other command & control servers to understand how widely FinFisher might be used. Claudio Guarnieri at Rapid7 (one of the authors of this report) was the first to search for these servers. He fingerprinted the Bahrain server and looked at historical Internet scanning data to identify other servers around the world that responded to the same fingerprint. Rapid7 published this list of servers, and described their fingerprinting technique. Other groups, including CrowdStrike and SpiderLabs also analyzed and published reports on FinSpy.

Immediately after publication, the servers were apparently updated to evade detection by the Rapid7 fingerprint. We devised a different fingerprinting technique and scanned portions of the internet. We confirmed Rapid7's results, and also found several new servers, including one inside Turkmenistan's Ministry of Communications. We published our list of servers in late August 2012, in addition to an analysis of mobile phone versions of FinSpy. FinSpy servers were apparently updated again in October 2012 to disable this newer fingerprinting technique, although it was never publicly described.

Nevertheless, via analysis of existing samples and observation of command & control servers, we managed to enumerate yet more fingerprinting methods and continue our survey of the internet for this surveillance software. We describe the results in this post.

Civil society groups have found cause for concern in these findings, as they indicate the use of FinFisher products by countries like Turkmenistan and Bahrain with problematic records on human rights, transparency, and rule of law. In an August 2012 response to a letter from UK-based NGO Privacy International, the UK Government revealed that at some unspecified time in the past, it had examined a version of FinSpy, and communicated to Gamma that a license would be required to export that version outside of the EU. Gamma has repeatedly denied links to spyware and servers uncovered by our research, claiming that the servers detected by our scans are "*not ... from the FinFisher product line*."[4] Gamma also claims that the spyware sent to activists in Bahrain was an "old" demonstration version of FinSpy, stolen during a product presentation.

In February 2013, Privacy International, the European Centre for Constitutional and Human Rights (ECCHR), the Bahrain Center for Human Rights, Bahrain Watch, and Reporters Without Borders filed a complaint with the Organization for Economic Cooperation and Development (OECD), requesting that this body investigate whether Gamma violated OECD Guidelines for Multinational Enterprises by exporting FinSpy to Bahrain.

The complaint called previous Gamma statements into question, noting that at least two different versions (4.00 and 4.01) of FinSpy were found in Bahrain, and that Bahrain's server was a FinFisher product and was likely receiving updates from Gamma. This complaint, as laid out by Privacy International states that Gamma:

- failed to respect the internationally recognised human rights of those affected by [its] activities
- caused and contributed to adverse human rights impacts in the course of [its] business activities
- failed to prevent and mitigate adverse human rights impacts linked to [its] activities and products, and failed to address such impacts where they have occurred
- failed to carry out adequate due diligence (including human rights due diligence); and
- failed to implement a policy commitment to respect human rights.

According to recent reporting, German Federal Police appear to have plans to purchase and use the FinFisher suite of tools domestically within Germany.[5] Meanwhile, findings by our group and others continue to illustrate the global proliferation of FinFisher's products. Research continues to uncover troubling cases of FinSpy in countries with dismal human rights track records, and politically repressive regimes. Most recently, work by Bahrain Watch has confirmed the presence of a Bahraini FinFisher campaign, and further contradicted Gamma's public statements. This post adds to the list by providing an updated list of FinSpy Command & Control servers, and describing the FinSpy malware samples in the wild which appear to have been used to target victims in Ethiopia and Vietnam.

We present these updated findings in the hopes that we will further encourage civil society groups and competent investigative bodies to continue their scrutiny of Gamma's activities, relevant export control issues, and the issue of the global and unregulated proliferation of surveillance malware.

FINFISHER: UPDATED GLOBAL SCAN

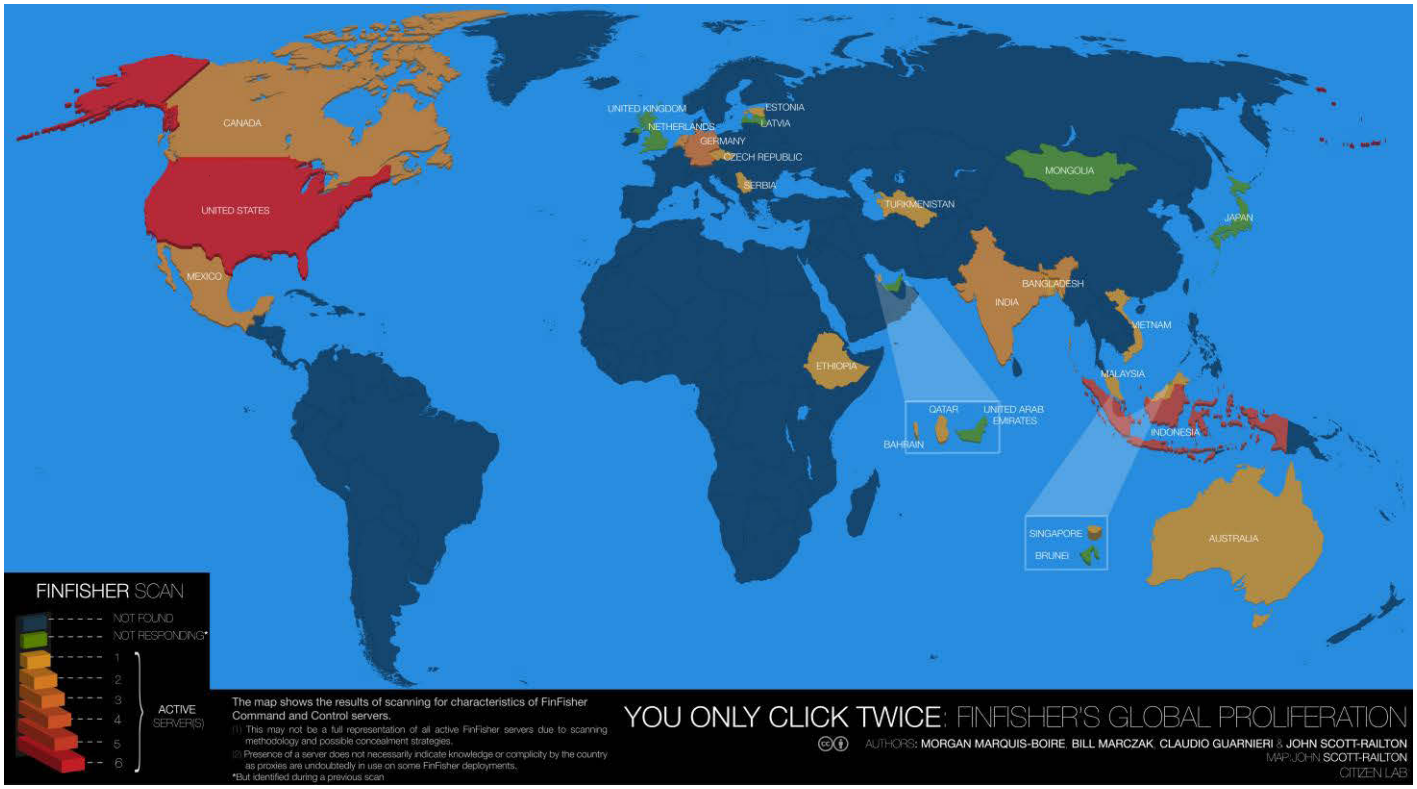


Figure 1. Map of global FinFisher proliferation

Around October 2012, we observed that the behavior of FinSpy servers began to change. Servers stopped responding to our fingerprint, which had exploited a quirk in the distinctive FinSpy wire protocol. We believe that this indicates that Gamma either independently changed the FinSpy protocol, or was able to determine key elements of our fingerprint, although it has never been publicly revealed.

In the wake of this apparent update to FinSpy command & control servers, we devised a new fingerprint and conducted a scan of the internet for FinSpy command & control servers. This scan took roughly two months and involved sending more than 12 billion packets. Our new scan identified a total of 36 FinSpy servers, 30 of which were new and 6 of which we had found during previous scanning. The servers operated in 19 different countries. Among the FinSpy servers we found, 7 were in countries we hadn't seen before.

New Countries
Canada, Bangladesh, India, Malaysia, Mexico, Serbia, Vietnam

In our most recent scan, 16 servers that we had previously found did not show up. We suspect that after our earlier scans were published the operators moved them. Many of these servers were shut down or relocated after the publication of previous results, but before the apparent October 2012 update. We no longer found FinSpy servers in 4 countries where previous scanning identified them (Brunei, UAE, Latvia, and Mongolia). Taken together, FinSpy servers are currently, or have been present, in 25 countries.

Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam.

Importantly, we believe that our list of servers is incomplete due to the large diversity of ports used by FinSpy servers, as well as other efforts at concealment. Moreover, discovery of a FinSpy command and control server in a given country is not a sufficient indicator to conclude the use of FinFisher by that country's law enforcement or intelligence agencies. In some cases, servers were found running on facilities provided by commercial hosting providers that could have been purchased by actors from any country.

The table below shows the FinSpy servers detected in our latest scan. We list the full IP address of servers that have been previously publicly revealed. For active servers that have not been publicly revealed, we list the first two octets only. Releasing complete IP addresses in the past has not proved useful, as the servers are quickly shut down and relocated.

IP	Operator	Routed to Country
117.121.xxx.xxx	GPLHost	Australia
77.69.181.162	Batelco ADSL Service	Bahrain
180.211.xxx.xxx	Telegraph & Telephone Board	Bangladesh
168.144.xxx.xxx	Softcom, Inc.	Canada
168.144.xxx.xxx	Softcom, Inc.	Canada
217.16.xxx.xxx	PIPNI VPS	Czech Republic
217.146.xxx.xxx	Zone Media UVS/Nodes	Estonia
213.55.99.74	Ethio Telecom	Estonia
80.156.xxx.xxx	Gamma International GmbH	Germany
37.200.xxx.xxx	JiffyBox Servers	Germany

178.77.xxx.xxx	HostEurope GmbH	Germany
119.18.xxx.xxx	HostGator	India
119.18.xxx.xxx	HostGator	India
118.97.xxx.xxx	PT Telkom	Indonesia
118.97.xxx.xxx	PT Telkom	Indonesia
103.28.xxx.xxx	PT Matrixnet Global	Indonesia
112.78.143.34	Biznet ISP	Indonesia
112.78.143.26	Biznet ISP	Indonesia
117.121.xxx.xxx	GPLHost	Malaysia
187.188.xxx.xxx	Iusacell PCS	Mexico
201.122.xxx.xxx	UniNet	Mexico
164.138.xxx.xxx	Tilaa	Netherlands
164.138.28.2	Tilaa	Netherlands
78.100.57.165	Qtel – Government Relations	Qatar
195.178.xxx.xxx	Tri.d.o.o / Telekom Srbija	Serbia
117.121.xxx.xxx	GPLHost	Singapore
217.174.229.82	Ministry of Communications	Turkmenistan
72.22.xxx.xxx	iPower, Inc.	United States
166.143.xxx.xxx	Verizon Wireless	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
117.121.xxx.xxx	GPLHost	United States
183.91.xxx.xxx	CMC Telecom Infrastructure Company	Vietnam

Several of these findings are especially noteworthy:

- Eight servers are hosted by provider GPLHost in various countries (Singapore, Malaysia, Australia, US). However, we observed only six of these servers active at any given time, suggesting that some IP addresses may have changed during our scans.
- A server identified in Germany has the registrant "Gamma International GmbH," and the contact person is listed as "Martin Muench."
- There is a FinSpy server in an IP range registered to "Verizon Wireless." Verizon Wireless sells ranges of IP addresses to corporate customers, so this is not necessarily an indication that Verizon Wireless itself is operating the server, or that Verizon Wireless customers are being spied on.
- A server in Qatar that was previously detected by Rapid7 seems to be back online after being unresponsive during the last round of our scanning. The server is located in a range of 16 addresses registered to "Qtel – Corporate accounts – Government Relations." The same block of 16 addresses also contains the website http://qhotels.gov.qa/.

3. ETHIOPIA AND VIETNAM: IN-DEPTH DISCUSSION OF NEW SAMPLES

3.1 FinSpy in Ethiopia

We analyzed a recently acquired malware sample and identified it as FinSpy. The malware uses images of members of the Ethiopian opposition group, Ginbot 7, as bait. The malware communicates with a FinSpy Command & Control server in Ethiopia, which was first identified by Rapid7 in August 2012. The server has been detected in every round of scanning, and remains operational at the time of this writing. It can be found in the following address block run by Ethio Telecom, Ethiopia's state-owned telecommunications provider:

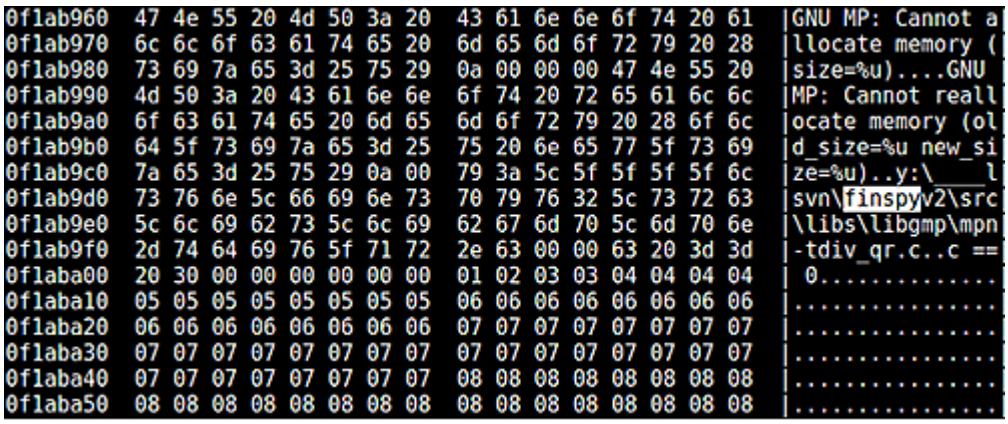
```
IP: 213.55.99.74
route: 213.55.99.0/24
descr: Ethio Telecom
origin: AS24757
mnt-by: ETC-MNT
member-of: rs-ethiotelecom
source: RIPE # Filtered
```

The server appears to be updated in a manner consistent with other servers, including servers in Bahrain and Turkmenistan.

MD5	8ae2febe04102450fdbc26a38037c82b
SHA-1	1fd0a268086f8d13c6a3262d41cce13470886b09
SHA-256	ff6f0bcdb02a9a1c10da14a0844ed6ec6a68c13c04b4c122afc559d606762fa

The sample is similar to a previously analyzed sample of FinSpy malware sent to activists in Bahrain in 2012. Just like Bahraini samples, the malware relocates itself and drops a JPG image with the same filename as the sample when executed by an unsuspecting user. This appears to be an attempt to trick the victim into believing the opened file is not malicious. Here are a few key similarities between the samples:

- The PE timestamp "2011-07-05 08:25:31" of the packer is exactly the same as the Bahraini sample.
- The following string (found in a process infected with the malware), self-identifies the malware and is similar to strings found in the Bahraini samples:



- The samples share the same Bootkit, SHA-256: ba21e452ee5ff3478f21b293a134b30ebf6b7f4ec03f8c8153202a740d7978b2.
- The samples share the same driverw.sys file, SHA-256: 62bde3bac3782d36f9f2e56db097a4672e70463e11971fad5de060b191efb196.

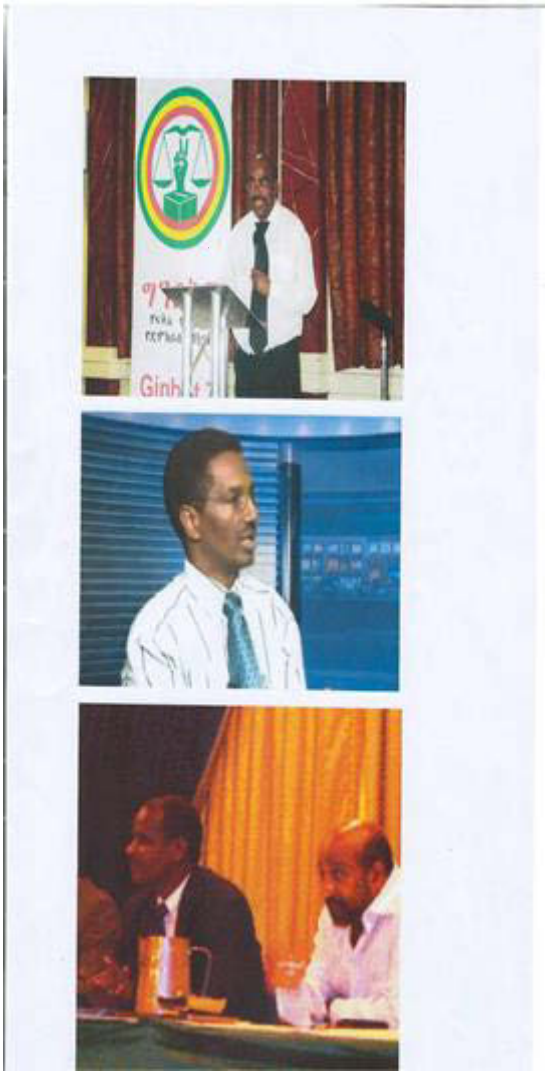


Figure 2. The image shown to the victim contains pictures of members of the Ginbot 7 Ethiopian opposition group

In this case the picture contains photos of members of the Ethiopian opposition group, Ginbot 7. Controversially, Ginbot 7 was designated a terrorist group by the Ethiopian Government in 2011. The Committee to Protect Journalists (CPJ) and Human Rights Watch have both criticized this action, CPJ has pointed out that it is having a chilling effect on legitimate political reporting about the group and its leadership.

The existence of a FinSpy sample that contains Ethiopia-specific imagery, and that communicates with a still-active command & control server in Ethiopia strongly suggests that the Ethiopian Government is using FinSpy.

3.2 FinSpy Mobile in Vietnam

We recently obtained and analyzed a malware sample[6] and identified it as FinSpy Mobile for Android. The sample communicates with a command & control server in Vietnam, and exfiltrates text messages to a Vietnamese telephone number.

The FinFisher suite includes mobile phone versions of FinSpy for all major platforms including iOS, Android, Windows Mobile, Symbian and Blackberry. Its features are broadly similar to the PC version of FinSpy identified in Bahrain, but it also contains mobile-specific features such as GPS tracking and functionality for silent 'spy' calls to snoop on conversations near the phone. An in-depth analysis of the FinSpy Mobile suite of backdoors was provided in an earlier blog post: [The Smartphone Who Loved Me: FinFisher Goes Mobile?]

MD5	573ef0b7ff1dab2c3f785ee46c51a54f
SHA-1	d58d4f6ad3235610bafba677b762f3872b0f67cb
SHA-256	363172a2f2b228c7b00b614178e4ffa00a3a124200ceef4e6d7edb25a4696345

The sample included a configuration file[7] that indicates available functionality, and the options that have been enabled by those deploying it:

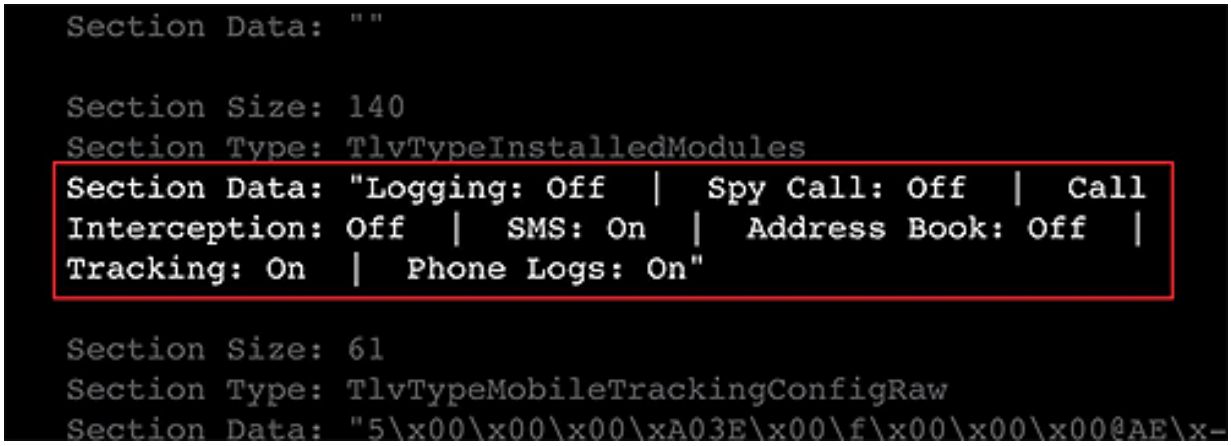


Figure 3. Image of a section of a configuration file for the FinSpy Mobile sample

Interestingly, the configuration file also specifies a Vietnamese phone number used for SMS based command and control:

Section Type: TlvTypeConfigSMSPhoneNumber
Section Data: "+841257725403"

The command and control server is in a range provided by the CMC Telecom Infrastructure Company in Hanoi:

IP Address: 183.91.2.199
inetnum: 183.91.0.0 – 183.91.9.255
netname: FTTX-NET
country: Vietnam
address: CMC Telecom Infrastructure Company
address: Tang 3, 16 Lieu Giai str, Ba Dinh, Ha Noi

This server was active until very recently and matched our signatures for a FinSpy command and control server. Both the command & control server IP and the phone number used for text-message exfiltration are in Vietnam which indicates a domestic campaign.

This apparent FinSpy deployment in Vietnam is troubling in the context of recent threats against online free expression and activism. In 2012, Vietnam introduced new censorship laws amidst an ongoing harassment, intimidation, and detention campaign against of bloggers who spoke out against the regime. This culminated in the trial of 17 bloggers, 14 of whom were recently convicted and sentenced to terms ranging from 3 to 13 years.[8]

4. BRIEF DISCUSSION OF FINDINGS

Companies selling surveillance and intrusion software commonly claim that their tools are only used to track criminals and terrorists. FinFisher, VUPEN and Hacking Team have all used similar language.[9] Yet a growing body of evidence suggests that these tools are regularly obtained by countries where dissenting political activity and speech is criminalized. Our findings highlight the increasing dissonance between Gamma's public claims that FinSpy is used exclusively to track "bad guys" and the growing body of evidence suggesting that the tool has and continues to be used against opposition groups and human rights activists.

While our work highlights the human rights ramifications of the mis-use of this technology, it is clear that there are broader concerns. A global and unregulated market for offensive digital tools potentially presents a

novel risk to both national and corporate cyber-security. On March 12th, US Director of National Intelligence James Clapper stated in his yearly congressional report on security threats:

"…companies develop and sell professional-quality technologies to support cyberoperations–often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target U.S. systems."

The unchecked global proliferation of products like FinFisher makes a strong case for policy debate about surveillance software and the commercialization of offensive cyber-capabilities.

Our latest findings give an updated look at the global proliferation of FinSpy. We identified 36 active FinSpy command & control servers, including 30 previously-unknown servers. Our list of servers is likely incomplete, as some FinSpy servers employ countermeasures to prevent detection. Including servers discovered last year, we now count FinSpy servers in 25 countries, including countries with troubling human rights records. This is indicative of a global trend towards the acquisition of offensive cyber-capabilities by non-democratic regimes from commercial Western companies.

The Vietnamese and Ethiopian FinSpy samples we identified warrant further investigation, especially given the poor human rights records of these countries. The fact that the Ethiopian version of FinSpy uses images of opposition members as bait suggests it may be used for politically influenced surveillance activities, rather than strictly law enforcement purposes.

The Ethiopian sample is the second FinSpy sample we have discovered that communicates with a server we identified by scanning as a FinSpy command & control server. This further validates our scanning results, and calls into question Gamma's claim that such servers are "*not … from the FinFisher product line*."[10] Similarities between the Ethiopian sample and those used to target Bahraini activists also bring into question Gamma International's earlier claims that the Bahrain samples were stolen demonstration copies.

While the sale of such intrusion and surveillance software is largely unregulated, the issue has drawn increased high-level scrutiny. In September of last year, the German foreign minister, Guido Westerwelle, called for an EU-wide ban on the export of such surveillance software to totalitarian states.[11] In a December 2012 interview, Marietje Schaake (MEP), currently the rapporteur for the first EU strategy on digital freedom in foreign policy, stated that it was "quite shocking" that Europe companies continue to export repressive technologies to countries where the rule of law is in question.[12]

We urge civil society groups and journalists to follow up on our findings within affected countries. We also hope that our findings will provide valuable information to the ongoing technology and policy debate about surveillance software and the commercialisation of offensive cyber-capabilities.

ACKNOWLEDGEMENTS

We'd like to thank Eva Galperin and the Electronic Frontier Foundation (EFF), Privacy International, Bahrain Watch, and Drew Hintz.

MEDIA COVERAGE

Media coverage of the report includes HuffingtonPost Canada, Salon, The Verge, Bloomberg Business Week, TheYoungTurks.

FOOTNOTES

[1]https://www.gammagroup.com/
[2]Software Meant to Fight Crime Is Used to Spy on Dissidents, http://goo.gl/GDRMe, New York Times, August 31, 2012, Page A1 Print edition.
[3]Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma, http://goo.gl/nJH7o, Bloomberg, July 25, 2012
[4]http://bits.blogs.nytimes.com/2012/08/16/company-denies-role-in-recently-uncovered-spyware/
[5]http://www.sueddeutsche.de/digital/finfisher-entwickler-gamma-spam-vom-staat-1.1595253
[6]This sample has also been discussed by Denis Maslennikov from Kasperksy in his analyses of FinSpy Mobile – https://www.securelist.com/en/analysis/204792283/Mobile_Malware_Evolution_Part_6
[7]Configuration parsed with a tool written by Josh Grunzweig of Spider Labs – http://blog.spiderlabs.com/2012/09/finspy-mobile-configuration-and-insight.html
[8]https://www.eff.org/deeplinks/2013/01/bloggers-trial-vietnam-are-part-ongoing-crackdown-free-expression
[9]https://www.securityweek.com/podcast-vupen-ceo-chaouki-bekrar-addresses-zero-day-marketplace-controversy-cansecwest
[10]http://bits.blogs.nytimes.com/2012/08/16/company-denies-role-in-recently-uncovered-spyware/
[11]http://www.guardian.co.uk/uk/2012/nov/28/offshore-company-directors-military-intelligence
[12]http://www.vieuws.eu/foreign-affairs/digital-freedoms-marietje-schaake-mep-alde/

Exhibit C

Exhibit C

[redacted]

ወንድምህ በብቃቱና በችሎታው በውጪ ጉዳይ ሚኒስቴር በከፍተኛ የሃላፊነት ደረጃ ሲሰራ ቆይቶ አሁንም መንግስቱን ወክሎ የአንድ ታላቅ አገር ኢትዮጵያ አምባሳደር በመሆን ሃገሩንና ወገኑን በከፍተኛ ብቃት እያገለገለ ነው፡፡ የኢትዮጵያ መንግስት መመዘኛ እከሌ ወንድሙ የት አለ? ምን ይሰራል? የሚለው ሳይሆን ብቃትና ችሎታ ብቻ መሆኑን ከዚህ የበለጠ ማረጋገጫ የምታገኝ አይመስለኝም፡፡ አንተ ከገባህበት የጥፋት መንገድ ተመልሰህ ከኛ ጋር ለመስራት ተስማምተህ አድራሻ ተለዋውጠን የተወሰነ እንቅስቃሴ ጀምረን ስናበቃ የገባኸውን ቃል አጥፈህ በሰራኸው ስህተት ቤተሰቦችህ እንዲገላቱ ከማድረግ በስተቀር ከድርጅቱም በኩል እምነትን አላተረፍክም፡፡ ቤተሰቦችህን ይዘህ ለንደን ድረስ በመሄድ “ሚስቴና ልጆቼ በወያኔ ታስረው ከኢትዮጵያ እንዲባረሩ ተደረገ ብለህ” አለቆችህን ለማሳመን ያደረከው ከንቱ ድካም ውጤት አላገኘህበትም፡፡ አሁን ባለው ሁኔታ ከእኛም ከእነሱም ሳትሆን ባዶ ሜዳ ላይ መቅረትህን ለመረዳት የምትቸገር አይመስለኝም፡፡
የጀመርከውን ስራ ለመቀጠል አሁንም ዕድሉ ዝግ አይደለም፡፡ ወደ ትክክለኛው ሰላማዊ መንገድ ለመመለስ ጊዜው አላለፈም፡፡ ፈቃደኛ ካልሆንክ ግን በተከታታይ የከፋ ጉዳት እንደሚደርስብህ ልታውቅ ይገባል፡፡ መጨረሻ ላይ ይህን መልእክት ለሌሎች አሳልፈህ በመስጠት ምናልባት ታማኝነትን አገኛለሁ በሚል ሌላ ስህተት እንዳትሰራ ደግሜ እያሳሰብኩህ አሁንም ምላሽህን በሚቀጥሉት 24 ሰዓታት ውስጥ እጠብቃለሁ፡፡
ሰገድ

Translation Services

[redacted]

Your brother held a high positon at the ministry of foreign affairs as a high ranking official as a result of his qualifications. He still serves the ministry and his country and fellow countrymen. Right now he serves his country and fellow citizens as an Ethiopian Ambasador in a prominant country. The Ethiopian government does not ask as to who is his brother or what his brother is doing? but the government judges him on his own merit alone. You cannot find any better evidence about the actions of the government other than this.

After you have agreed to come out of the wrong way you were in and agreed to work with us and exchanged addresses, started some activities, you broke your promises on your own mistake. You did not get trust even from the organization, you only made your family suffer. You took your family to London and complained by saying " Woyane [TPLF] imprisoned my wife and children and expelled them." This ineffective efort did not gain you the trust of your bosses. I do not think that you will have difficulty to understand that you are losing from us and them and that you are left alone.

The door is not yet closed to continue that assignment that you have started. It is not late to come back to the peaceful way. If you are not willing to cooperate with us, you should know that you will suffer from continuos and major attack. At last, I advise you not to make another mistake by passing this message to others in an anticipation of getting their trust. I warn you and ask you to contact me within the next 24 hours. I am waiting for your response.

Seged.

Subscribed and sworn to before me, this 10th day of February 2014 a Notary Public in and for the State of Maryland

Notary Public

My commission expires 12/30 20 17

ooo End of Translation ooo

CERTIFICATE OF TRANSLATION AND ACCURACY

Pursuant to 8 C.F.R. § 1003.33, I, Dinberu Melakehiwot, duly sworn upon oath, depose and certify that I am competent to translate the attached document from Amharic to English. I further certify that the foregoing translation is true and accurate to the best of my knowledge and abilities.

Signature of Translator: ----------

የትክክለኛ ትርጉም ማረጋገጫ ሰርተፊኬት

በአሜሪካ መንግስት የፌደራል መንግስት ህግ አንቀፅ 8 የስደተኞች እና የዜግነት ክፍል ቁጥር 8ሲ ኤፍ አር 1003.33(8CFR 1003.33) መሰረት እኔ ድንበሩ መላከሕይወት የአማርኛ እና የእንግሊዘኛ ቋንቋዎች ሙሉ እውቀት ያለኝ ከመሆኑም በላይ በዚህ ቋንቋዎች ሙሉ በሙሉ መተርጎም እችላለሁ። ከዚህ በላይ የተመለከተዉን የእንግሊዘኛ መረጃ በትክክል የተረጎምኩ መሆኑን አረጋግጣለሁ። ከዚህ በተጨማሪም ይህ ትርጉም እውነተኛ እና ትክክለኛ መሆኑን አረጋግጣለሁ።

የተርጓሚው ፊርማ ----------

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

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

Pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, Defendant Federal Democratic Republic of Ethiopia ("Ethiopia") hereby moves this Court to dismiss Plaintiff John Doe, a.k.a. Kidane's ("Plaintiff") First Amended Complaint (Doc. No. 26). As set forth in the accompanying Memorandum, this Court lacks subject matter jurisdiction because Ethiopia is a foreign sovereign, which, under the Foreign Sovereign Immunities Act ("FSIA"), is immune from suit, unless Plaintiff can demonstrate that the suit falls within a specified statutory exception to immunity. Here, the sole exception – the "tort" exception – on which Plaintiff relies, does not apply. Accordingly, Ethiopia retains its immunity and this Court lacks subject matter jurisdiction.

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

WHEREFORE, for these reasons, as well as those set forth in the accompanying memorandum, Ethiopia respectfully requests that the Court dismiss Plaintiff's First Amended Complaint, with prejudice.[1]

Dated: August 4, 2014

Respectfully submitted,

/s/ Robert P. Charrow

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

Counsel for Defendant Federal Democratic Republic of Ethiopia

[1] By filing this motion, accompanying memorandum, and proposed order, Ethiopia is not waiving its sovereign immunity.

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

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

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

Counsel for Defendant Federal Democratic Republic of Ethiopia

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTRODUCTION AND SUMMARY OF ARGUMENT. 1

SUMMARY OF THE COMPLAINT. 5

ARGUMENT 6

I. ETHIOPIA, AS A FOREIGN SOVEREIGN, IS PRESUMPTIVELY IMMUNE FROM SUIT 6

II. THE TORT EXCEPTION DOES NOT APPLY TO THE ALLEGATIONS IN THE AMENDED COMPLAINT 7

A. The Tort Exception Does Not Apply Where, As Here, the Entirety of the Alleged Tort was Not Committed in the United States. 7

B. The Tort Exception Does Not Apply to the Discretionary Functions Alleged in the Amended Complaint 11

C. The Tort Exception Does Not Apply to Claims Based on Deceit, as Alleged in the Amended Complaint. 13

D. The Tort Exception Does not Apply to Statutory Damages or to Injuries for Annoyance, as Alleged in the Amended Complaint 14

E. The Tort Exception Does Not Apply to Either Violations of the Wiretap Act or Common Law "Intrusion Upon Seclusion". 15

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

a. The Interception Provision of the Wiretap Act Does Not Apply to Sovereigns. 15

b. The Amended Complaint Fails to Allege a Necessary "Interception" to Support a Wiretap Act Claim. 17

2. Plaintiff Has Not and Cannot Plead Intrusion Upon Seclusion 19

a. The Amended Complaint Does Not Allege that Defendant Intentionally Intruded on Plaintiff's Seclusion. 19

b. Common Law Torts, Such as Intrusion Upon Seclusion, Are Expressly Preempted by the Wiretap Act. 20

CONCLUSION.....21

TABLE OF AUTHORITIES

Cases

Antares Aircraft L.P. v. Federal Republic of Nigeria,
1991 WL 29287 (S.D.N.Y. Mar. 1, 1991). 8

Argentine Republic v. Amerada Hess Shipping Corp.,
488 U. S. 428 (1989)....6, 8

Ashcroft v. Iqbal,
556 U.S. 662 (2009)....15

Asociacion de Reclamantes v. United Mexican States,
735 F.2d 1517 (D.C. Cir. 1984). 6, 7

Bailer v. Erie Ins. Exch.,
344 Md. 515, 687 A.2d 1375 (1997). 19

Bell Atlantic Corp. v. Twombly,
550 U.S. 544 (2007)....15

Bruce v. Consulate of Venezuela,
No. 04-933 (RWR) (D.D.C. Aug. 31, 2005)....13

Bunnell v. Motion Picture Ass'n of America,
567 F. Supp. 2d 1148 (C.D. Cal. 2007) 20

Burnett v. Al Baraka Invest. and Dev. Corp.,
292 F.Supp.2d 9 (D.D.C. 2003). 13

Cargill Int'l S.A. v. M/T Pavel Dybenko,
991 F.2d 1012 (2d Cir. 1993)....7

City of Ontario, Cal. v. Quon,
560 U.S. 746 (2010)....20

City of Los Angeles v. Lyons,
461 U.S. 95 (1983)....21

Coleman v. Alcolac, Inc.,
888 F.Supp. 1388 (S.D.Tex.1995). 8

Dalehite v. United States,
346 U.S. 15 (1953)....11

Darcars Motors of Silver Spring, Inc. v. Borzym,
150 Md. App. 8, 818 A.2d 1159 (2003).....9

De Sanchez v. Banco Central De Nicaragua,
770 F.2d 1385 (5th Cir. 1985). 11

Doe v. Chao,
540. U.S. 614 (2004)..15

F.A.A. v. Cooper,
566 U.S. ___, 132 S. Ct. 1441 (2012).....14

Four Corners Helicopters, Inc. v. Turbomeca S.A.,
677 F.Supp. 1096 (D. Col.1988).....8

Fraser v. Nationwide Mut. Ins. Co.,
352 F.3d 107 (3d Cir. 2003).....17, 18

Haven v. Polska,
215 F.3d 727 (7th Cir. 2000). 14

In re Lett,
238 B.R. 167 (Bankr. W.D. Mo. 1999).....9

Jerez v. Republic of Cuba,
777 F.Supp.2d 6 (D.D.C. 2011). 7

Jin v. Ministry of State Security,
475 F.Supp.2d 54 (D.D.C. 2007). 13

Konop v. Hawaiian Airlines,
302 F.3d 868 (9th Cir. 2002). 18

Lane v. CBS Broadcasting Inc.,
612 F. Supp. 2d 623 (E.D. Pa. 2009). 21

Lane v. Pena,
518 U.S. 187 (1996).....14

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992).....21

MacArthur Area Citizens Ass'n v. Republic of Peru,
809 F.2d 918 (D.C. Cir. 1987). 12

O'Bryan v. Holy See,
556 F.3d 361 (6th Cir. 2009). 7, 8, 10, 11

Persinger v. Islamic Republic of Iran,
729 F.28 835 (D.C. Cir. 1984) 3, 7

Phoenix Consulting, Inc. v. Republic of Angola,
216 F.3d 36 (D.C. Cir. 2000). 6

Price v. Socialist People's Libyan Arab Jamahiriya,
294 F.3d 82 (D.C. Cir. 2002). 16

Quon v. Arch Wireless Operating Co., Inc.,
445 F. Supp. 2d 1116 (C.D. Cal. 2006) 20

Risk v. Halvorsen,
936 F.2d 393 (9th Cir. 1991). 13

Ruggiero v. Compania Peruana de Vapores "Inca Capac Yupanqui,"
639 F.2d 872 (2d Cir. 1981).....2

Sheldon ex rel. Olsen v. Government of Mexico,
729 F.2d 641 (9th Cir. 1984). 11

Steve Jackson Games, Inc. v. United States Secret Serv.,
36 F.3d 457 (5th Cir. 1994) 18

Theofel v. Farey–Jones,
359 F.3d 1066 (9th Cir. 2004). 17

TIFA, Ltd. v. Republic of Ghana,
CIV.A. 88-1513, 1991 WL 179098 (D.D.C. Aug. 27, 1991). 13, 14

United States v. Councilman,
418 F.3d 67 (1st Cir. 2005). 18

United States v. Gaubert,
499 U.S. 315 (1991).....12

United States v. S.A. Empresa De Viacao Aerea Rio Grandense (Varig Airlines),
467 U.S. 797 (1984).....11, 12

United States v. Steiger,
318 F.3d 1039 (11th Cir.). 17, 18, 19

Valentine v. NebuAd, Inc.,
804 F. Supp. 2d 1022 (N.D. Cal. 2011). 21

Verlinden B. V. v. Central Bank of Nigeria,
461 U. S. 480 (1983)....6

Vermont Agency of Natural Res. v. United States ex rel. Stevens,
529 U.S. 765 (2000)....16

Von Dardel v. Union of Soviet Socialist Republics,
736 F. Supp. 1 (D.D.C. 1990). 7

Wye Oak Tech., Inc. v. Republic of Iraq,
941 F.Supp.2d 53 (D.D.C. 2013)....1

Statutes

18 U.S.C. § 2510....16, 17

18 U.S.C. § 2511....16

18 U.S.C. § 2517....17

18 U.S.C. § 2518....4, 21

18 U.S.C. § 2520(a). 16

28 U.S.C. § 1330 ....2, 3, 6, 7, 11, 17

28 U.S.C. § 1331....2

28 U.S.C. § 1367....2

28 U.S.C. § 1604....3, 6

28 U.S.C. § 1605(a) 2, 3, 4, 7, 8, 9, 11, 13

28 U.S.C. § 2680(a) 11

Rules

Fed. R. Civ. P. 12(b)(1)....1, 3, 17

Fed. R. Civ. P. 12(b)(2)....16

Fed. R. Civ. P. 12(b)(6)....1, 4, 17

Other Authorities

BLACK'S LAW DICTIONARY 405 (6th ed. 1990). 14

Press Release, Electronic Frontier Foundation, American Sues Ethiopian Government for Spyware Infection (Feb. 18, 2004). 2, 3

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

Joseph Dellapenna, *Suing Foreign Governments and Their Corporations,* 1st ed., The Bureau of National Affairs: Washington, D.C. (1988). 6

H. Rep. 94-1497(1976). 8

S. Rep. No. 94-938 (1976). 14

RESTATEMENT (SECOND) OF TORTS (1977). 15

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

Introduction & Summary of Argument:

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

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

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

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

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

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

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

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

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

---

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

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

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

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

Summary of the Complaint:

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

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

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

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

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

Argument:

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

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

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

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

> in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment; except this paragraph shall not apply to—
>
> > (A)any claim based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused, or
> >
> > (B)any claim arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights

28 U. S. C. § 1605(a)(5).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Under the Wiretap Act, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action

recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2520(a) (emphasis supplied). Here, the anonymous Plaintiff alleges that Defendant violated section 2511 "by [the] unlawful interception of Plaintiff's communications." FAC at ¶¶ 15 and 91. No other provisions of the Wiretap Act are referenced in the Complaint. The "interception" provision of section 2511(1) reads as follows:

> Except as otherwise specifically provided in this chapter any person who—
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

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

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

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

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

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

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

"Interception" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). "The Circuits which have interpreted this definition as applied to electronic communications have held that it encompasses only acquisitions contemporaneous with transmission." *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir.), *cert. denied*, 538 U.S. 1051 (2003) (collecting cases from Fifth and Ninth Circuits) (emphasis supplied). *See Theofel v. Farey–Jones*, 359 F.3d 1066, 1077–78 (9th Cir. 2004) (post-delivery); *Fraser v.*

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

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

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

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

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

2. Plaintiff Has Not and Cannot Plead Intrusion Upon Seclusion

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

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

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

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

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

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

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

> The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications."

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

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

Conclusion:

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

Dated: August 4, 2014

Respectfully submitted,

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

Counsel for Defendant Federal Democratic Republic of Ethiopia

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

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

TABLE OF CONTENTS

Table of Authorities ii

Introduction 1

Statement of the Case 4

Argument 6

I. Ethiopia bears the burden of proving immunity from suit under the FSIA 6

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. 8

A. The tort exception applies to violations of the Wiretap Act and common law intrusion upon seclusion. 8

1. Ethiopia's recording of Plaintiff's Skype calls unambiguously violated the Wiretap Act. 8

2. Ethiopia's monitoring of Plaintiff's Web usage was an unambiguous intrusion upon his seclusion 13

B. The tort exception applies because Ethiopia wiretapped a U.S. citizen in the privacy of his home on U.S. soil. 15

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. 21

1. Ethiopia's agents had no discretion to commit criminal wiretapping in violation of federal law. 22

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. 24

D. Mr. Kidane's tort claims are based on Defendant's affirmative misconduct, not misrepresentation or deceit. 26

E. Mr. Kidane's claim for intrusion upon seclusion is not preempted by the Wiretap Act. 29

F. Injunctive relief is available under the FSIA 32

G. Intrusion upon seclusion constitutes a personal injury 33

Conclusion 34

TABLE OF AUTHORITIES

Cases

Adams v. City of Battle Creek,
250 F.3d 980 (6th Cir. 2001) 10, 11, 12

Agudas Chasidei Chabad of U.S. v. Russian Fed'n,
729 F. Supp. 2d 141 (D.D.C. 2010) 32

Am. Nat'l Ins. Co. v. FDIC,
642 F.3d 1137 (D.C. Cir. 2011) 7

Am. Online, Inc. v. Nat'l Health Care Disc., Inc.,
121 F. Supp. 2d 1255 (N.D. Iowa 2000) 17

Antares Aircraft L.P. v. Fed. Republic of Nigeria,
No. 89 CIV. 6513(JSM), 1991 WL 29287 (S.D.N.Y. Mar. 1, 1991) 21

Argentine Republic v. Amerada Hess Shipping Corp.,
488 U.S. 428 (1989) 6, 15, 20

Asociacion de Reclamantes v. United Mexican States,
735 F.2d 1517 (D.C. Cir. 1984) 15

Bell Helicopter Textron Inc. v. Islamic Republic of Iran,
764 F. Supp. 2d 122 (D.D.C. 2011),
vacated on other grounds, 892 F. Supp. 2d 219 (D.D.C. 2012) 32

Bernstein v. Nat'l Broad. Co.,
129 F. Supp. 817 (D.D.C. 1955)
aff'd, 232 F.2d 369 (D.C. Cir. 1956) 34

Birnbaum v. United States,
588 F.2d 319 (2d Cir. 1978) 24

Black v. Sheraton Corp. of Am.,
564 F.2d 531 (D.C. Cir. 1977) 28

Bodunde v. Parizek,
93 C 1464, 1993 WL 189941 (N.D. Ill. May 28, 1993) 13

Burnett v. Al Baraka Invest. & Dev. Corp.,
292 F. Supp. 2d 9 (D.D.C. 2003) 23

Coleman v. Alcolac, Inc.,
888 F. Supp. 1388 (S.D. Tex. 1995) 21

Conner v. Tate, 130 F. Supp. 2d 1370 (N.D. Ga. 2001) 11, 12, 13

Cruikshank v. United States,
431 F. Supp. 1355 (D. Haw. 1977) 24

De Sanchez v. Banco Central de Nicaragua,
515 F. Supp. 900 (E.D. La. 1981) 28

De Sanchez v. Banco Central de Nicaragua,
770 F.2d 1385 (5th Cir. 1985) 28

Doe v. Bin Laden,
663 F.3d 64 (2d Cir. 2011) 19

Doe v. Holy See,
557 F.3d 1066 (9th Cir. 2009) 23

Dorris v. Absher,
959 F. Supp. 813 (M.D. Tenn. 1997)
aff'd in part, rev'd in part, 179 F.3d 420 (6th Cir. 1999) 11, 13

Dresbach v. Doubleday & Co., Inc.,
518 F. Supp. 1285 (D.D.C. 1981) 33

Four Corners Helicopters, Inc. v. Turbomeca S.A.,
677 F. Supp. 1096 (D. Col. 1988) 21

Garza v. Bexar Metro. Water Dist.,
639 F. Supp. 2d 770 (W.D. Tex. 2009) 11, 12

George v. Carusone,
849 F. Supp. 159 (D. Conn. 1994) 18

Gulf Res. Am., Inc. v. Republic of Congo,
370 F.3d 65 (D.C. Cir. 2004) 1, 6

Hatahley v. United States,
351 U.S. 173 (1956) 24

In re NSA Telecomm. Records Litig.,
564 F. Supp. 2d 1109 (N.D. Cal. 2008) 25

In re Premises Located at 840 140th Ave. NE, Bellevue, Wash.,
634 F.3d 557 (9th Cir. 2011) 25

In re SEDCO, Inc.,
543 F. Supp. 561 (S.D. Tex. 1982) 20

In re State Police Litig.,
888 F. Supp. 1235 (D. Conn. 1995) 18

In re Terrorist Attacks on September 11, 2001,
349 F. Supp. 2d 765 (S.D.N.Y. 2005)
on reconsideration in part, 392 F. Supp. 2d 539 (S.D.N.Y. 2005) 23

Jacobson v. Rose,
592 F.2d 515 (9th Cir. 1978) 18

Jerez v. Republic of Cuba,
777 F. Supp. 2d 6 (D.D.C. 2011) 20

Jin v. Ministry of State Sec.,
475 F. Supp. 2d 54 (D.D.C. 2007) 23

Kyllo v. United States,
533 U.S. 27 (2001) 19

Lane v. CBS Broad., Inc.,
612 F. Supp. 2d 623 (E.D. Penn. 2009) 30

Leong v. Carrier IQ, Inc.,
2012 U.S. Dist. LEXIS 59480 (C.D. Cal. Apr. 27, 2012) 29, 30, 31

Letelier v. Republic of Chile,
488 F. Supp. 665 (D.D.C. 1980) 19, 23

Liu v. Republic of China,
892 F.2d 1419 (9th Cir. 1989) 18, 19, 23

MacArthur Area Citizens Ass'n v. Republic of Peru,
809 F.2d 918 (D.C. Cir. 1987),
modified on other grounds, 823 F.2d 606 (D.C. Cir. 1987) 19, 22, 23

New Summit Assocs. Ltd. P'ship v. Nistle,
533 A.2d 1350 (Md. App. 1987) 16

Niedermayer v. Adelman,
90 B.R. 146 (D. Md. 1988).....33

O'Bryan v. Holy See,
556 F.3d 361 (6th Cir. 2009) 21, 28

Olsen v. Gov't of Mexico,
729 F.2d 641 (9th Cir. 1984). 18, 20

Organizacion JD Ltda. v. U.S. Dep't of Justice,
18 F.3d 91 (2d Cir. 1994) 11, 12

Orlikow v. United States,
682 F. Supp. 77 (D.D.C. 1988) 24

Pascale v. Carolina Freight Carriers Corp.,
898 F. Supp. 276 (D.N.J. 1995).....10

PBA Local No. 38 v. Woodbridge Police Dep't,
832 F. Supp. 808 (D.N.J. 1993).....11

Pearce v. E.F. Hutton Grp., Inc.,
664 F. Supp. 1490 (D.D.C. 1987) 33, 34

Persinger v. Islamic Republic of Iran,
729 F.2d 835 (D.C. Cir. 1984).....20

Risk v. Halvorsen,
936 F.2d 393 (9th Cir. 1991) 23

Sanders v. Robert Bosch Corp.,
38 F.3d 736 (4th Cir.1994) 9

Schuchart v. La Taberna del Alabardero, Inc.,
365 F.3d 33, 35–36 (D.C. Cir. 2004).....27

Sheppard v. Google, Inc.
2012 U.S. Dist. LEXIS 173184 (W.D. Ark. Dec. 6, 2012).....30, 31

Shively v. Carrier IQ, Inc.,
No. C-12–0290 EMC, 2012 U.S. Dist. LEXIS 103237, 2012 WL 3026553, at (N.D. Cal. July 24, 2012) 31

Snyder v. Phelps,
533 F. Supp. 2d 567 (D. Md. 2008),
rev'd on other grounds, 580 F.3d 206 (4th Cir. 2009),
aff'd on other grounds, 131 S. Ct. 1207 (U.S. 2011) 33

Tifa, Ltd. v. Republic of Ghana,
No. 88–CV-1513, 1991 U.S Dist. LEXIS 11855 (D.D.C. Aug. 27, 1991) 27

United States v. Cotroni,
527 F.2d 708 (2d Cir. 1975) 15

United States v. Gaubert,
499 U.S. 315 (1991) 22

United States v. Ivanov,
175 F. Supp. 2d 367 (D. Conn. 2001) 17

United States v. McLemore,
28 F.3d 1160 (11th Cir. 1994) 12

United States v. Nelson,
837 F.2d 1519 (11th Cir. 1988) 10, 16

United States v. Rodriguez,
968 F.2d 130 (2d Cir. 1992) 16, 18

United States v. Turk,
526 F.2d 654 (5th Cir. 1976) 10, 16

Valentine v. Nebuad, Inc.,
804 F. Supp. 2d 1022 (N.D. Cal. 2011) 30

Van Dardel v. Union of Soviet Socialist Republics,
736 F. Supp. 1 (D.D.C. 1990) 20

Williams v. City of Tulsa. OK,
393 F. Supp. 2d 1124 (N.D. Okla. 2005) 10, 11, 12

Statutes

18 U.S.C. § 1030(a)(4) 17
18 U.S.C. § 2510....25
18 U.S.C. § 2510(4) 9, 16
18 U.S.C. § 2511....10
18 U.S.C. § 2511(2)(f) 25
18 U.S.C. § 2511(a) 23
18 U.S.C. § 2518(10) 29
18 U.S.C. § 2518(10)(c)....29
18 U.S.C. § 2520....10, 11, 12
18 U.S.C. § 2707(a) 12
28 U.S.C § 1605(a)(5) 7, 32
28 U.S.C. § 1602....19
28 U.S.C. § 1605(a)(5)(A)....21
28 U.S.C. § 1605(a)(5)(B) 26, 27, 28
28 U.S.C. § 1606....32
28 U.S.C. § 2680(a) 21
28 U.S.C. § 2680(h)....28
28 U.S.C. §§ 1330....6
28 U.S.C. §§ 1602–1611....6
50 U.S.C. § 1801....25

Other Authorities

Restatement (Second) of Torts § 652B 27
U.S. Dep't of State, "Treaties and Agreements" 2012 8
U.S. Dept. of State Foreign Affairs Manual, 7 FAM 960 Criminal Matters (2013) ...25

U.S. Congress

147 Cong. Rec. H. 7159, 7198 (Oct. 23, 2001)....12
147 Cong. Rec. S. 10990, 11007 (Oct. 25, 2001)....12
S. Rep. No. 541, 99th Cong., 2d Sess. 43 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3597 13
S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555....19, 26

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

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

DEFENDANT'S REPLY TO PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION TO DISMISS FIRST AMENDED COMPLAINT PURSUANT TO RULES 12(b)(1) and 12(b)(6) OF THE FEDERAL RULES OF CIVIL PROCEDURE

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

Counsel for Defendant Federal Democratic Republic of Ethiopia

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTRODUCTION AND SUMMARY OF ARGUMENT. 1

ARGUMENT 5

I. PLAINTIFF CONCEDES THAT THE ENTIRE TORT DID NOT OCCUR IN THE UNITED STATES AND THEREFORE, UNDER THE LAW OF THIS CIRCUIT, ETHIOPIA'S IMMUNITY REMAINS INTACT 5

II. SPYING IS A DISCRETIONARY FUNCTION AND, THEREFORE, THE TORT EXCEPTION DOES NOT APPLY 10

III. THE TORT EXCEPTION DOES NOT APPLY TO TORTS THAT INVOLVE, AS HERE, TRICKERY OR DECEIT. 11

IV. PLAINTIFF CONCEDES THAT THE TORT EXCEPTION DOES NOT APPLY TO HIS CLAIM FOR STATUTORY DAMAGES. 11

V. DEFENDANT HAS NOT AND CANNOT VIOLATE THE INTERCEPTION PROVISION OF THE WIRETAP ACT 12

A. A Foreign State Is Not a "Person" Within the Meaning of the Wiretap Act. 12

B. Plaintiff Has Failed to Allege An Interception 15

VI. PLAINTIFF HAS FAILED TO ALLEGE A VIOLATION OF INTRUSION UPON SECLUSION. 15

A. Plaintiff Has Failed to Plead the Requisite Intent. 15

B. Intrusion Upon Seclusion is Preempted. 17

VII. PLAINTIFF CONCEDES THAT HE IS NOT ENTITLED TO A JURY TRIAL OR TO DECLARATORY RELIEF, AND THE FSIA FORECLOSES INJUNCTIVE RELIEF. 18

CONCLUSION 19

TABLE OF AUTHORITIES

Cases

Adams v. City of Battle Creek,
250 F.3d 980 (6th Cir. 2001). 14

Agudas Chasidei Chabad of U.S. v. Russian Federation,
528 F.3d 944 (D.C. Cir. 2008). 5

Antares Aircraft L.P. v. Federal Republic of Nigeria,
1991 WL 29287 (S.D.N.Y. Mar. 1, 1991). 7

Asociacion de Reclamantes v. United Mexican States,
735 F.2d 1517 (D.C. Cir. 1984). 6, 7, 9

Bailer v. Erie Ins. Exch.,
344 Md. 514, 687 A.2d 1375 (1997). 16

Baska v. Scherzer,
283 Kan. 750, 156 P.3d 617 (2007). 16

Black v. Sheraton Corp. of Am.,
564 F.2d 531 (D.C. Cir. 1977). 11

Bourne v. Mapother & Mapother, P.S.C.,
2014 WL 555130 (S.D. W.Va. Feb. 12, 2014). 16

Cabiri v. Gov't of the Republic of Ghana,
165 F.3d 193 (2d Cir. 1999)....11

Catawba Cnty., N.C. v. EPA,
571 F.3d 20 (D.C. Cir. 2009). 14

City of Los Angeles v. Lyons,
461 U.S. 95 (1983). 18

Coleman v. Alcolac, Inc.,
888 F.Supp. 1388 (S.D.Tex.1995). 6

Collier v. District of Columbia,
2014 WL 2256908 (D.D.C. May 30, 2014). 16

Elam v. Kansas City Southern Railway Co.,
635 F.3d 796 (5th Cir. 2011). 17

F.A.A. v. Cooper,
566 U.S. ___, 132 S. Ct. 1441 (2012).....11, 12

Four Corners Helicopters, Inc. v. Turbomeca S.A.,
677 F.Supp. 1096 (D. Col.1988).....6, 7

Gonzaga Univ. v. Doe,
536 U.S. 273 (2002).....13

Gubtch v. Fed. Republic of Germany,
444 F.Supp.2d 1 (D.D.C. 2006).....5

Haven v. Polska,
215 F.3d 727 (7th Cir. 2000).....12

In re Sedco, Inc.,
543 F.Supp. 561 (S.D. Tex. 1982).....6, 9

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

Keller v. Central Bank of Nigeria,
277 F.3d 811 (6th Cir. 2002).....5

Lane v. Pena,
518 U.S. 187 (1996).....11

Letelier v. Republic of Chile,
488 F. Supp. 665 (D.D.C. 1980).....9

Liu v Republic of China,
892 F.2d 1419 (9th Cir. 1989).....8, 9

Lugar v. Edmondson Oil Co.
457 U.S. 922 (1982).....13

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992).....18

Merrell Dow Pharmaceuticals, Inc. v. Thompson,
478 U.S. 804 (1986).....4, 18

Metropolitan Life Ins. Co. v. Taylor,
481 U.S. 58 (1987).....18

O'Bryan v. Holy See,
556 F.3d 361 (6th Cir. 2009). 6, 9, 10

Olsen v. Gov't of Mexico,
729 F.2d 641 (9th Cir. 1984). 8, 9

Pascale v. Carolina Freight Carriers Corp.,
898 F. Supp. 276 (D.N.J. 1995). 15

Persinger v. Islamic Republic of Iran,
729 F.28 835 (D.C. Cir. 1984) 6

Price v. Socialist People's Libyan Arab Jamahiriya,
294 F.3d 82 (D.C. Cir. 2002). 14

Riegel v. Medtronic, Inc.,
552 U.S. 312 (2008).. 17

Ruffin v. United States,
642 A.2d 1288 (D.C. 1994). 16

Rusello v. United States,
464 U.S. 16 (1982). 14

Samuels v. District of Columbia,
770 F.2d 184 (D.C. Cir. 1985). 13

Sanders v. Robert Bosch Corp.,
38 F.3d 736 (4th Cir. 1994). 15

United States v. Cotroni,
527 F.2d 708 (2d. Cir. 1975) 7

United States v. Nelson,
837 F.2d 1519 (11th Cir. 1988) 8

United States v. Rodriguez,
968 F.2d 130 (2d. Cir. 1992) 8

Vermont Agency of Natural Res. v. United States ex rel. Stevens,
529 U.S. 765 (2000) 13, 14

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

White Stallion Energy Ctr., LLC v. EPA,
748 F.3d 1222 (D.C. Cir 2014). 14

Statutes

18 U.S.C. § 2510. ..... 3, 8, 13, 14

18 U.S.C. § 2511. ..... 3, 4, 12, 13, 14

18 U.S.C. § 2518. 17

18 U.S.C. § 2520. ..... 3, 13, 14

42 U.S.C. § 1983. 13

28 U.S.C. § 1605(a). 11

National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495. ..... 2, 10

Rules

Fed. R. Civ. P. 8(a). 3

Fed. R. Civ. P. 12(b)(1). 3

Other Authorities

Ronald Dworkin, THE MODEL OF RULES I (1967). 7

H.L.A. Hart, THE CONCEPT OF LAW (1961). 7

DEFENDANT'S REPLY TO PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION TO DISMISS FIRST AMENDED COMPLAINT PURSUANT TO RULES 12(b)(1) and 12(b)(6) OF THE FEDERAL RULES OF CIVIL PROCEDURE

Introduction & Summary of Argument:

In this Foreign Sovereign Immunities Act ("FSIA") case, Plaintiff alleges that the Federal Democratic Republic of Ethiopia ("Ethiopia") intentionally infected from Ethiopia a friend's home computer with a virus and that that virus subsequently infected Plaintiff's computer after Plaintiff opened a document that he received from that friend, believing the document to be secure. Plaintiff further alleges that the computer virus, which was controlled by government employees in Ethiopia, enabled those employees in Ethiopia to read emails and other documents that he had received or produced on his home computer. As a result, he filed a two-count complaint alleging that Ethiopia violated the Federal Wiretap Act and committed the common law tort of intrusion upon seclusion.

Ethiopia moved to dismiss the First Amended Complaint ("FAC") because the tort exception to sovereign immunity does not apply for five reasons: (1) the alleged tort did not occur in its entirety in the United States, as required by the law of this Circuit; (2) the alleged spying is a discretionary activity and, therefore, not subject to the tort exception; (3) the tort exception does not apply to conduct involving deceit or trickery, as is alleged to be the case here; (4) the tort exception does not apply to "statutory damages," as claimed here; and (5) the tort exception does not apply because the FAC fails to allege a violation of either the Wiretap Act or the common law tort of intrusion upon seclusion. The interception provision of the Wiretap Act alleged to have been violated by Defendant only applies to "persons," and a foreign state is not a "person." Moreover, the FAC fails to allege an "interception," as that term has been defined by the courts. Correspondingly, Plaintiff does not allege that Defendant intentionally "intruded"

upon Plaintiff's seclusion, as required under Maryland law. To the contrary, the FAC alleges that Defendant intended to intrude upon the seclusion of another party not involved in this case. Finally, common law torts arising out of the same conduct proscribed by the Wiretap Act are preempted by that Act.

It is against this backdrop that Plaintiff concedes, as he must, that all of the human acts and the intent underlying both of the alleged torts occurred in Ethiopia. Plaintiff, relying on cropped passages from a D.C. Circuit case and a Ninth Circuit case argues that the non-human aspects of the tort occurred in the United States and that should be sufficient. The law of this Circuit is to the contrary--the entire tort must occur in the Unites States. Non-human conduct is simply not relevant. This is not disputed by Plaintiff and that should end this matter.

Plaintiff also argues that "spying" is not a discretionary function because wiretapping is a wrong under United States law. Whether certain actions are "wrong" under United States law is not the test for the discretionary function exemption. If it were, the exemption would never apply since every tort, by definition, is "a civil wrong." Moreover, whether judged by U.S. or international law, spying overseas, which is what is alleged to have occurred here, is perfectly legal and quintessentially discretionary. If spying overseas were otherwise, the Central Intelligence Agency would lack a legal foundation. *See* National Security Act of 1947, § 102.

Plaintiff alleges that Defendant has attempted to "recast" his complaint by alleging that the tortious conduct involves deception or trickery; torts that involve deception fall outside the tort exception to sovereign immunity. However, as Plaintiff begrudgingly acknowledges, the word "trick" is the Plaintiff's word, not the Defendant's invention. *See* FAC ¶ 41 ("In the case of the image, the target is tricked into opening the executable and is thus infected."); Exh. B at 8 (Doc. # 26 at 38) ("This appears to be an attempt to trick the victim into believing the opened file

is not malicious."). Recognizing that allegations of deception are not actionable, it is Plaintiff who is running from his own words.

Defendant also sought dismissal under Rule 12(b)(1) because the tort exception only applies, as relevant here, to claims for money damages for "personal injury." Plaintiff, in his Wiretap Act count, is seeking "statutory damages," rather than actual damages. Plaintiff does not take issue with this argument and, therefore, concedes that statutory damages are not authorized by the tort exception. As such, the Wiretap Act claim must be dismissed. As to the common law claim, Plaintiff belatedly alleges that he has suffered mental distress as a result of the alleged computer hacking, but fails to provide any detail in his FAC as required by Rule 8(a). The original complaint contained no allegation that he suffered mental distress. Plaintiff does not address this issue other than arguing that mental distress is a form of personal injury. Given that the burden to prove facts necessary to establish jurisdiction is on the plaintiff, and given that a bald assertion of an allegation without more is insufficient to carry that jurisdictional burden, Plaintiff's common law claim does not satisfy the tort exception.

Ethiopia argued that to satisfy the tort exception, Plaintiff must plead a tort. The provision of the Wiretap Act which forms the basis of Plaintiff's first count, only applies to "persons," and a foreign state is not a person. Instead of directly responding, Plaintiff sets up two straw men. First, he argues that many courts have held that domestic governmental units, *e.g.*, municipalities, are "persons" within the meaning of sections 2510 and 2511. However, those cases are irrelevant because section 2510 expressly defines "person" to include political units within a State of the Union; that definition, though, does not include foreign governments. Second, he argues that a foreign state is an entity and that section 2520 permits a civil action against an entity. The only problem there is that section 2520 creates no independent causes of

action; the sole statutory cause of action relied upon by Plaintiff is section 2511(1)(a), which is limited to "persons." The Wiretap Act also requires contemporaneous transmission; this did not occur here. Rather, the information, according to the FAC, was copied onto a file on Plaintiff's own computer and then, only later, transmitted to Ethiopia. Plaintiff's significant discussion of why as a matter of policy he ought to be entitled to proceed under the Wiretap Act underscores the fact that the words of the statute cannot carry the weight of his claims.

Plaintiff has not and cannot adequately plead a claim for intrusion upon seclusion for two reasons. First, the requisite intent is lacking. Plaintiff admits that he was not the intended victim of the hackers, but rather was collateral damage. Since he was not the alleged intended victim, Defendant had no intent to invade Plaintiff's computer. And absent that intent, there is no tort. The doctrine of transferred intent does not apply to invasion of privacy, or to an act and an intent that are not simultaneous, as is the case here. Also, the Wiretap Act expressly preempts common law remedies. Plaintiff responds by arguing that courts have held that the Act does not completely preempt state law. Plaintiff is confused. Complete preemption is a jurisdictional concept channeling cases automatically into federal court and ousting state courts of jurisdiction. Most federal statutes that preempt state laws involve "ordinary preemption" and do not "completely preempt" state law. *See Merrell Dow Pharmaceuticals, Inc. v. Thompson*, 478 U.S. 804 (1986) (holding that Food, Drug, and Cosmetic Act § 521, which preempts certain state laws, does not completely preempt state laws).

Finally, Plaintiff argues that he has discharged his burden of proof and that the burden has shifted to Ethiopia to demonstrate that it is entitled to immunity. The Plaintiff confuses the burden of proof with the burden of producing evidence. "The party claiming FSIA immunity bears the initial burden of proof of establishing a prima facie case that it satisfies the FSIA's

definition of a foreign state; once this prima facie case is established, the burden of production shifts to the non-movant to show that an exception applies." *Keller v. Central Bank of Nigeria*, 277 F.3d 811, 815 (6th Cir. 2002). The party claiming immunity under FSIA retains the burden of persuasion throughout this process. *See id*. The burden of proof, though, is only relevant where there are factual disputes. Here, aside from one pleading issue, Ethiopia has, for purposes of this motion, not challenged the factual accuracy of the FAC. Ethiopia does challenge the adequacy of Plaintiff's belated claim that he now suffers from emotional distress. In the Motion to Dismiss, Ethiopia challenged Plaintiff to provide additional detail to flesh out this assertion, which is necessary to establish jurisdiction for Plaintiff's invasion of seclusion claim. Under the law of this Circuit, though, "the plaintiff must, on a challenge by the defendant, present adequate supporting evidence." *Agudas Cahsidei Chabad of United States v. Russian Fed*., 528 F.3d 934, 940 (D.C. Cir. 2008). The burden to produce evidence thus shifted to Plaintiff to provide additional detail. None was provided and, therefore, Plaintiff has not met his jurisdictional burden.

Argument:

I. Plaintiff Concedes That the Entire Tort Did Not Occur in the United States and Therefore, Under the Law of this Circuit, Ethiopia's Immunity Remains Intact

Under the law of this and many other Circuits, the FSIA's tort exception is only satisfied if the entire tort occurred in the United States. *See e.g., Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1524–25 (D.C. Cir. 1984); *Gubtch v. Fed. Republic of Germany*, 444 F.Supp.2d 1, 11 (D.D.C. 2006) ("In addition, both the tortious act and the injury must occur in the United States for this exception to apply"). Plaintiff never directly challenges this statement of the law of this Circuit, but instead argues that "[t]he 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." Plaintiff's Opposition ("Opp.") at 15. From this, Plaintiff ordains a so-called "essential locus" test and then applies this new test to the facts as alleged in the FAC. The only problem is that the "essential locus" test is not used in this or any other circuit. Specifically, the Court in *Asociacion de Reclamantes* stated that

> [e]ven if the allegedly wrongful failure to compensate had the effect of retroactively rendering the prior acts on United States soil tortious, at the very least the entire tort would not have occurred here, *see In re Sedco, Inc*., 543 F.Supp. 561, 567 (S.D.Tex.1982) ("the tort, in whole, must occur in the United States"), and indeed we think its essential locus would remain Mexico.

Asociacion de Reclamantes, 735 F.2d at 1525 (emphasis supplied). Under *Asociacion* and its progeny the "entire tort" must occur in the United States. Plaintiff does not address these cases other than arguing that the law of the Circuit should be ignored because in those cases, the torts occurred overseas. But that is precisely the point: the Courts have consistently held that the entire tort must occur in the United States to satisfy the exception. Any case in which some or all of the tort occurred overseas is, by definition, a tort that is not subject to the FSIA's tort exception, even though the injury may have occurred in the United States. *See Von Dardel v. Union of Soviet Socialist Republics*, 736 F. Supp. 1, 7 (D.D.C. 1990); *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d at 1525 ("The tort, in whole, must occur in the United States") (quoting *In re Sedco, Inc*., 543 F. Supp. 561, 567 (S.D. Tex. 1982)); *Persinger v. Islamic Republic of Iran*, 729 F.2d 835, 842 (D.C. Cir.1984), *cert. denied*, 469 U.S. 881 (1984) (same): *Jerez v. Republic of Cuba*, 777 F.Supp.2d 6, 25 (D.D.C. 2011) (same); *see also O'Bryan v. Holy See*, 556 F.3d 361, 382 (6th Cir. 2009) (where the Sixth Circuit "join[ed] the Second and D.C. Circuits in concluding that in order to apply the tortious act exception, the 'entire tort' must occur in the United States."); *Coleman v. Alcolac, Inc.,* 888 F.Supp. 1388, 1403 (S.D.Tex.1995) (exception not applicable because alleged tort "did not occur wholly in this country"); *Four*

Corners Helicopters, Inc. v. Turbomeca S.A., 677 F.Supp. 1096, 1102 (D. Col.1988) ("It is clear that in order for the exception to apply, the entire tort must have occurred in the United States"); *Antares Aircraft L.P. v. Federal Republic of Nigeria*, 1991 WL 29287 (S.D.N.Y. Mar. 1, 1991) ("It is well-recognized that for the non-commercial tort exception to apply, the entire tort must occur in the U.S.") (*aff'd on other grounds*, 948 F.2d 90 (2d Cir. 1991), *vacated mem.*, 505 U.S. 1215 (1992), *aff'd on other grounds*, 999 F.2d 33 (2d Cir. 1993)).

Rather than confronting the law of the Circuit, Plaintiff presents the law as he believes it ought to be, rather than as it is. While the dichotomy between the law as it is and the law as it ought to be has been the subject of lively debates in the jurisprudential literature, it is decidedly out of place when it comes to applying the law of the Circuit to resolve whether a district court has subject matter jurisdiction over a particular claim. *Compare* H.L.A. Hart, THE CONCEPT OF LAW (1961) *with* Ronald Dworkin, THE MODEL OF RULES I (1967).

Under Plaintiff's view of the law, the tort exception ought to apply even if most of the tort occurs overseas. In an attempt to give his "ought" a bit more of the "is," Plaintiff relies on a series of non-FSIA wiretap cases and three FSIA cases--two from the Ninth Circuit and one from this Court antedating this Circuit's ruling in *Asociacion de Reclamantes v. United Mexican States* and its progeny. The various wiretap cases are not instructive.

The concept that the entire tort must occur in the United States is an outgrowth of the Supreme Court and the Circuit Courts' interpretation of the tort exception in the FSIA. Cases dealing with other statutory regimes are therefore not relevant. For example, Plaintiff cites *United States v. Cotroni,* 527 F.2d 708, 711 (2d. Cir. 1975), for the proposition that "the situs of the Wiretap Act violation is the place where the interception occurs." Opp. at 15. But, that is not what *Cotroni* says. *Cotroni* stands for the proposition that the Wiretap Act does not have

extraterritorial application, and it clarifies that whether the Wiretap Act applies depends on where the "interception" took place. But, it neither interprets the term "interception," nor defines the "situs" of a Wiretap Act violation. Correspondingly, in *United States v. Rodriguez*, 968 F.2d 130, 136 (2d. Cir. 1992), the Court found that because the definition of interception encompasses the "aural" acquisition of the contents of the communication, "the interception must also be considered to occur at the place where the redirected contents are first heard." *United States v. Rodriguez*, 968 F.2d 130, 136 (2d. Cir. 1992). The Court held that "there is no indication in the legislative history that [Congress] intended to extinguish the principle that the place where the contents of a wire communication are first to be heard and understood by human ears, other than those of the parties to the conversation, is the situs of an interception within the meaning of Section 2510(4)." *Id.* Applying *Rodriguez* to the instant case, the situs of the interception was both in the United States, where Plaintiff contends FinSpy captured the contents of Plaintiff's communications, and Ethiopia, where the recordings allegedly were heard. Thus, the tort was not "committed entirely" in the United States, and under the law of this Circuit, the tort exception cannot apply. *United States v. Nelson,* 837 F.2d 1519 (2d. Cir. 1992), is inapposite because it applies to determinations about whether a lawful warrant has been issued, not determinations about whether a tort exists.

Moreover, none of the three FSIA cases relied upon by Plaintiff does the trick: none adopts the so-called "essential locus" test either. The two Ninth Circuit cases, *Olsen v. Gov't of Mexico*, 729 F.2d 641, 646 (9th Cir. 1984) and *Liu v. Republic of China*, 892 F.2d 1419, 1434 (9th Cir. 1989), do not advance Plaintiff's novel "locus" theory. In *Olsen,* decedents, who were imprisoned in Mexico, were being flown on a plane owned by the Mexican government to the United States where they could serve the remainder of their sentence. En route from Mexico, the

plane, while attempting to land in the United States, crashed near San Diego, California. The Court found that one complete tort--negligent piloting--occurred in the United States; the concept of the tort's locus was never mentioned by the court. In *Liu,* plaintiff's husband was allegedly murdered in the United States by an employee of the Republic of China. The entire tort occurred in the United States; the court applied the employee tort exception because it found that the employee had acted within the course and scope of his employ thereby satisfying the "employee" tort exception. Here, plaintiff has not alleged that any Ethiopian employee acted in the United States as was the case in both *Olsen* and *Liu*. Finally, Plaintiff invokes *Letelier v. Republic of Chile*, 488 F. Supp. 665 (D.D.C. 1980), but, again in that case the entire tort, a double assassination, was perpetrated in Washington, D.C. by agents of Chile. Here, unlike in *Olsen*, *Liu* or *Letelier*, none of the acts occurred in the United States, no agent or employee of Ethiopia was physically present in the United States and none of the equipment was housed or operated in the United States. Here, aside from the alleged injury, none of the allegedly tortious conduct occurred in this country.

Having been unable to find any FSIA case supporting his novel locus theory, Plaintiff is left to argue that this Court should ignore the *Asociacion de Reclamantes* Court's reliance on *In re Sedco,* because *Sedco* is 32 years old and comes from a court outside this district. The fact that *Sedco* was cited with approval by this Circuit should end this matter; its age is not relevant. Finally, as an afterthought and in a footnote, Plaintiff suggests that *O'Bryan v. Holy See*, 556 F.3d 361 (6th Cir. 2009), is irrelevant because "Plaintiff brings no claims alleging negligent training or supervision in Ethiopia." Opp. at 21, n. 37. Under that constrained view, *Olsen* would not be relevant because Plaintiff brings no claims alleging negligent piloting. *O'Bryan v. Holy See* involved torts that had their effect through employees in the United States, but the

negligent actions allegedly occurred in Vatican City. The Sixth Circuit, relying on the Second and D.C. Circuits, held that the entire tort must occur in the United States and, therefore, dismissed the claims for negligent supervision or training.

Here, like in *Holy See*, all of the actors performed their allegedly tortious actions overseas and even though those actions allegedly injured individuals in the United States, since the entire tort did not occur in the United States the tort exception to sovereign immunity does not apply.

II. Spying is a Discretionary Function and, Therefore, the Torts Exception Does Not Apply

Actions that are discretionary are not subject to the tort exception to sovereign immunity. Plaintiff argues that since wiretapping is a wrong and since no one has discretion to commit a wrong, the discretionary function exemption cannot apply. First, plaintiff's argument would read the discretionary function exception out of the statute. The only time the exception is relevant is when a sovereign has allegedly committed a wrong. If tortious activity is automatically deemed non-discretionary, it would defeat the purpose of the exception. Second, Plaintiff is correct in noting that certain types of criminal activity, namely activities that violate universal norms, such as murder and torture, cannot support a discretionary function exemption. But, that is not what is alleged here. As even Plaintiff acknowledges, the legality of the activity is not the test, but rather whether the activity violates universal norms. Spying overseas is not viewed with the universal scorn necessary to obviate the discretionary function exemption. To the contrary, it is perfectly proper under U.S. law for the United States to spy on another nation and to spy on the residents of that other nation. The Central Intelligence Agency is authorized by the National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495, to conduct, as appropriate, overseas intelligence activities. Thus, the actions that Plaintiff accuses Ethiopia of having undertaken, namely spying abroad, is entirely proper under United States law. Plaintiff has provided nothing to indicate that

Ethiopian law is to the contrary. Third, spying is inherently discretionary, a fact not contested by Plaintiff, especially whereas here, it is alleged to have occurred because of Plaintiff's friend's political views.

III. The Tort Exception Does Not Apply to Torts that Involve, as Here, Trickery or Deceit

Plaintiff alleges that his claims are not based on misrepresentation or deceit because neither of the torts he alleges requires him to prove misrepresentation or deceit as an element. That, however, is not the test. Rather, one looks to the Plaintiff's complaint to assess whether "the wrongful acts alleged to have caused the injury" involve misrepresentations. *Cabiri v. Gov't of the Republic of Ghana*, 165 F.3d 193, 200 (2d Cir. 1999). Here, the cascade of events that Plaintiff alleges caused him injury was the result of trickery. Indeed, spyware, by its very nature works only through trickery. Plaintiff alleges that he was tricked into opening what appeared to be a benign document from a friend that contained the hidden spyware at issue. Plaintiff has pled trickery, a form of deceit, and he cannot now run from it.

Plaintiff, relying on *Black v. Sheraton Corp. of Am.*, 564 F.2d 531, 541 (D.C. Cir. 1977), a Federal Tort Claims Act ("FTCA") case involving improper government eavesdropping, suggests that because this case was permitted to proceed under the FTCA, then eavesdropping somehow does not involve "deceit." However, there is nothing to indicate that plaintiff there ever alleged that he was deceived or tricked by the government; that is not the case here. The issue of deceit was never raised by any of the parties or addressed by the court. The case, while of historical interest as the last of the "Bobby Baker" cases, is irrelevant here.

IV. Plaintiff Concedes That the Tort Exception Does Not Apply to His Claim for Statutory Damages

The tort exception, as relevant here, only applies to claims for money damages "for personal injury or death." § 1605(a)(5). Exceptions to sovereign immunity are strictly construed. *See F.A.A.*

v. Cooper, 566 U.S. ___, 132 S. Ct. 1441, 1448 (2012); *Lane v. Pena*, 518 U.S. 187, 192 (1996); *see also Haven v. Polska,* 215 F.3d 727, 731 (7th Cir. 2000) (noting that FSIA exceptions must be "narrowly construed" because they are "in derogation of the common law"). Here, Plaintiff "seeks statutory damages under the Wiretap Act." FAC at ¶ 12. Plaintiff does not dispute this and therefore concedes that his claim for "statutory damages" is not cognizable under the tort exception to the FSIA. Since a claim for "money damages" for "personal injury" is the only relevant remedy permitted under the tort exception and since Plaintiff is not claiming damages for "personal injury" under the Wiretap Act, the tort exception does not apply to his Wiretap Act claim.

V. Defendant Has Not and Cannot Violate the Interception Provisions of the Wiretap Act

Plaintiff must demonstrate that defendant has committed a tort to sustain subject matter jurisdiction under the tort exception. Plaintiff claims that defendant violated the "interception" provision of the Wiretap Act at 18 U.S.C. § 2511. Indeed, Plaintiff's first cause of action is entitled "Violation of the Wiretap Act, 18 U.S.C. § 2511."

A. A Foreign State Is Not a "Person" Within the Meaning of the Wiretap Act

In its Motion to Dismiss, Ethiopia argued that a foreign sovereign cannot violate 18 U.S.C. § 2511, because that section only applies to "persons" and a foreign sovereign is not a "person."

Section 2511 provides in relevant part as follows:

> (1) Except as otherwise specifically provided in this chapter any person who—
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication
>
> * * *
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

Plaintiff argues that because section 2520, which authorizes a civil action for any violation of any provision of the Wiretap Act, uses the terms "person" or "entity," and since an entity can include a country, the Wiretap Act necessarily applies to Defendant.

The problem, though, is that section 2520 itself creates no substantive rights. Rather, it simply provides a cause of action to vindicate rights identified in other portions of the Wiretap Act, specifically communications "intercepted, disclosed, or intentionally used in violation of this chapter. " § 2520(a) (emphasis added). In this sense, § 2520 is like 42 U.S.C. § 1983. *See Gonzaga Univ. v. Doe,* 536 U.S. 273 (2002); *Lugar v. Edmondson Oil Co*., 457 US 922, 924 (1982); *Samuels v. District of Columbia*, 770 F.2d 184, 193 (D.C. Cir. 1985) ("By its terms, of course, [section 1983] does not create substantive rights; instead it provides an express federal remedy against state officials for deprivations of rights established elsewhere in federal law."). Thus, a court must look to the scope and nature of the specific substantive right Plaintiff accuses Defendant of violating to determine whether Plaintiff may assert that right against a foreign state. Here, Plaintiff accuses Ethiopia of violating the interception provision of the Wiretap Act, 18 U.S.C. §2511(1)(a), which, as noted above, prohibits "any person" from intentionally intercepting any wire, oral, or electronic communication. Thus, § 2511(1) protects only against actions taken by a "person" as defined in the statute, which does not include foreign states. Indeed, section 2510(6) defines the word "person" to mean "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." Conspicuously absent from this overarching definition is the phrase "foreign nation" or "foreign state." Giving the statute its plain meaning is consistent with the "longstanding interpretive presumption that 'person' does not include the sovereign." *Vermont Agency of Natural Res. v. United States ex rel. Stevens*, 529

U.S. 765, 780-81 (2000); *see also Price v. Socialist People's Libyan Arab Jamahiriya*, 294 F.3d 82, 96 (D.C. Cir. 2002) ("[W]e hold that foreign states are not 'persons' protected by the Fifth Amendment.").

Instead of examining whether section 2511 encompasses a foreign state, Plaintiff string cites cases examining whether a city or municipality is "a political subdivision" of a State, as those terms are used in section 2511. *See, e.g., Adams v. City of Battle Creek*, 250 F.3d 980 (6th Cir. 2001); Opp. at 10-12. None of the cases in the string cite holds that a foreign state is a "person" within the meaning of either section 2510 or section 2511. Plaintiff goes on to argue that "this Court should follow those courts that have held that the legislative history supports constructing the statute to impose civil liability on governmental entities." Opp. at 13. But those courts were only examining whether section 2511 should be interpreted to reach U.S. municipalities and comparable domestic governmental units. We are unaware of any case holding that the term "person" under section 2511 includes a foreign sovereign and the Plaintiff has cited to none.

Finally, Plaintiff argues that the use of the words "person" and "entity" in section 2520 is dispositive because entity includes a governmental actor. However, as noted above, section 2510, which creates Plaintiff's cause of action, only uses the word "person." It does not use the word "entity." "Where Congress includes particular language [such as the word 'entity'] in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally…in the disparate inclusion or exclusion." *White Stallion Energy Ctr., LLC v. EPA.,* 748 F.3d 1222, 1238 (D.C. Cir. 2014) (quoting *Rusello v. United States*, 464 U.S. 16, 23 (1982)); *cf. Catawba Cnty., N.C. v. EPA*, 571 F.3d 20, 36 (D.C. Cir. 2009). Accordingly, Courts must assume that Congress intended to omit the word "entity" from section 2511.

B. Plaintiff Has Failed to Allege An "Interception"

Defendant, in its motion to dismiss, noted that according to majority view, the interception provision of the Wiretap Act requires that the interception of the communication occur at the same time as the transmission. Here, Plaintiff argues that that is not the law and that interception can occur if a defendant records the conversation at the time it was occurring. Those cases though assume that the defendant recorded the conversation on some equipment installed by the defendant. *See, e.g.*, *Sanders v. Robert Bosch Corp.*, 38 F.3d 736 (4th Cir. 1994) (defendant recorded using a "voice logger"); *Pascale v. Carolina Freight Carriers Corp.*, 898 F. Supp. 276 (D.N.J. 1995) (recording via "tape recording equipment" installed by the defendant). That is not the case here. As alleged in the FAC, the Skype conversations at issue were recorded onto Plaintiff's own computer, just like any other temporary file, the only difference is that spyware sought to camouflage those temporary files so they could not be easily detected. The information stored in those temporary files were subsequently allegedly transmitted to Defendant in Ethiopia, according to the FAC ¶ 10 ("FinSpy programs installed on the Kidane family computer in Maryland to create contemporaneous recording of his activities in Maryland, which the FinSpy programs then sent to the FinSpy Master server located in Ethiopia."). Given that there was no simultaneous transmission and no recording on another device, there was no interception within the meaning of the Wiretap Act.

VI. Plaintiff Has Failed to Allege a Violation of Intrusion Upon Seclusion

Ethiopia sought dismissal of count II, intrusion upon seclusion, on the grounds (i) that the FAC failed to allege the requisite intent and (ii) that tort was preempted by the Wiretap Act.

A. Plaintiff Has Failed to Plead the Requisite Intent

Under Maryland law, the tort of intrusion upon seclusion occurs when

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

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

This tort requires that there be an intent to "intrude . . .upon the seclusion of another" with liability flowing in favor of the "the other for the invasion of his privacy." Thus, the defendant's intended target of the intrusion must be the same as the party who is actually intruded upon.

Plaintiff responds by arguing that as long as Defendant intended to spy upon someone, that is all that is required. *See* Opp. 14. However, that assumes that the concept of transferred intent governs intrusion upon seclusion, as pled in this case. It does not. First, Defendant is unaware of any reported case applying transferred intent to intrusion upon seclusion, and Plaintiff has pointed to none. *See Bourne v. Mapother & Mapother, P.S.C.*, 2014 WL 555130 (S.D. W.Va. Feb. 12, 2014) (concluding that transferred intent does not apply to a claim for intentional infliction of emotional distress and finding it unnecessary to decide whether it applies to an invasion of privacy type tort). Second, transferred intent is "the principle that one who intends to injure one person and instead injures a bystander is liable for an intentional tort against the injured person. *See, e.g., Baska v. Scherzer*, 283 Kan. 750, 156 P.3d 617, 623, 628 (2007) (a plaintiff was injured when she stepped in the middle of a fist fight; while she was hit "unintentionally," transferred intent applied and her claim was for assault and battery); *see also Ruffin v. United States*, 642 A.2 1288, 1293 (D.C.1994) (transferred intent applies in context of criminal law)." *Collier v. District of Columbia*, CV 13-1790 (RMC), 2014 WL 2256908 (D.D.C. May 30, 2014). Transferred intent requires that the intent to injure a given party and the act that was intended to injure that party but which injured another party occur simultaneously. That

clearly is not the case here where the alleged intent to intrude into the computer of Plaintiff's friend and the alleged act of so intruding occurred long before the spyware made its way into Plaintiff's computer.

Plaintiff also argues that there was an ongoing "intrusion." However, the word "intrusion," by definition, is not a continuous activity any more than "breaking and entering" is continuous activity. Once you have broken and entered, the act has been completed and once you have "intruded" the act has been completed. The act of intruding must co-exist with the intent to intrude on a particular person; absent transferred intent, which is not applicable, there was no intent to intrude into Plaintiff's computer, and none is alleged.

B. Intrusion Upon Seclusion is Preempted

The Wiretap Act states as follows:

> (c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

18 U.S.C. § 2518(10).

Plaintiff spills much ink citing case after case to the effect that the Wiretap Act does not "completely preempt" state law. *See* Opp. at 30-31. Plaintiff's response is muddled since he confuses two concepts--"ordinary preemption" and "complete preemption"--that have little to do with each other. *See Elam v. Kansas City Southern Railway Co*., 635 F.3d 796, 803 (5th Cir. 2011) (discussing distinction between ordinary preemption and complete preemption). Ordinary preemption, which is at issue here, occurs where a federal law either expressly or by implication displaces a state law, including common law torts. *See Riegel v. Medtronic, Inc*., 552 U.S. 312 (2008) (Medical Device Amendments expressly preempt most tort actions). Preemption is an affirmative defense and may not be used as the basis to remove a case to federal court. *See*

Merrell Dow Pharmaceuticals, Inc. v. Thompson, 478 U.S. 804 (1986). In contrast, "complete preemption" is a jurisdictional doctrine. If a statute "completely preempts" state law, any claims under that state law are not only displaced but a state court also lacks any jurisdiction to entertain the case; jurisdiction is exclusively within the purview of the federal courts. The Employee Retirement Income Security Act of 1974 is an example of one of those rare laws that completely preempts state law. *See Metropolitan Life Ins. Co. v. Taylor*, 481 U. S. 58 (1987). Thus, the fact that the Wiretap Act does not completely preempt state law is irrelevant. It is one of many federal laws that have ordinary preemptive effect.

If the Court finds that the Defendant has violated the Wiretap Act, whether a remedy is available or not, then by the plain language of that Act, the Court must dismiss the common law claim because it is powerless to provide any remedy. Absent the ability to provide a remedy, a federal court lacks Article III jurisdiction. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Thus, by way of example, if this Court were to find that the Wiretap Act had been violated, but that the claim for statutory damages was insufficient to trigger the tort exception, the common law claim would be preempted by the clear language of the Wiretap Act.

VII. Plaintiff Concedes that He Is Not Entitled to a Jury Trial or to Declaratory Relief and the FSIA Forecloses Injunctive Relief

Plaintiff does not take issue with Ethiopia's arguments that neither a trial by jury nor declaratory relief is available under the FSIA. *See* Memorandum in Support of Motion to Dismiss at 2 n.1. Nor does he take issue with Ethiopia's argument that neither pendent nor diversity jurisdiction is available. *See id.* Those points are therefore conceded. However, Plaintiff now argues that he is entitled to injunctive relief even though such relief was never sought in the original complaint and even though he lacks standing under *City of Los Angeles v. Lyons*, 461 U.S. 95(1983) to seek such relief. Even if those impediments were not sufficient, the

tort exception only authorizes money damages. This Court lacks subject matter jurisdiction to entertain any relief other than money damages.

Conclusion:

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

Respectfully submitted,

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

Counsel for Defendant Federal Democratic Republic of Ethiopia

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

John Doe, Plaintiff,	) Civil Action) No. 14-cv-372)
vs.	) MOTION HEARING)
Federal Democratic Republic of Ethiopia, Defendant.	) Washington, DC) July 14, 2015) Time: 2:00 p.m.)

TRANSCRIPT OF MOTION HEARING
HELD BEFORE
THE HONORABLE JUDGE RANDOLPH D. MOSS
UNITED STATES DISTRICT JUDGE

A P P E A R A N C E S

For the Plaintiff:
Nathan Daniel Cardozo
Cindy Cohn
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Scott A. Gilmore
CENTER FOR JUSTICE & ACCOUNTABILITY
One Hallidie Plaza
Suite 406
San Francisco, CA 94102

For the Defendant:
Robert Phillip Charrow
Melissa Prusock
GREENBERG, TRAURIG, LLP
2101 L Street, NW
Suite 1000
Washington, DC 20037

Court Reporter:
Janice E. Dickman, RMR, CRR
Official Court Reporter
United States Courthouse, Room 6523
333 Constitution Avenue, NW
Washington, DC 20001
202-354-3267

THE COURTROOM DEPUTY: Civil action 14-372, John Doe versus the Federal Democratic Republic of Ethiopia.

Counsel, will you please approach the podium and identify yourselves for the record.

MR. CARDOZO: Good afternoon, Your Honor. Nathan Cardozo for the plaintiff John Doe, A/K/A Mr. Kidane. And with me I have my colleague Cindy Cohn and Scott Gilmore.

THE COURT: Good afternoon.

MR. CHARROW: Robert P. Charrow for the defendant Federal Republic. And with me is Miss Prusock, you just admitted.

THE COURT: Thank you again. Welcome. Just before getting going, one thing that I just wanted to put on the record, I don't think is an issue, but I always prefer full disclosure on these things, and if anyone sees an issue, please let me know. But when I was in private practice, not all that long ago, one of the opposing counsel in at least one of my cases was EFF.

And in addition, I think that Mr. Snider, who is one of the counsel representing the Federal Republic was at Wilmer, Cutler, Pickering, Hale and Dorr when I was there, as well. So, if anyone has any issue, please let know. But I'm not aware of any.

So, we're here for argument today on defendant's motion to dismiss. I think that given the number of issues

that are involved, that if the parties don't mind doing it this way, it would probably be most helpful for the court to proceed, at least, on an issue-by-issue basis with respect to the major issues. I think we could probably clump some of the issues together.

But I think that rather than having defendants go first and go through all the issues and then having the plaintiff then have to go back and respond to things that I may have heard oral argument about some time earlier, it may be easier to do it one issue at a time.

And I guess the issue where I would like to start would be with the discretionary function exception to the Foreign Sovereign Immunities Act. And, obviously, if there are any overview points that you want to make, you should feel free to make those at this time as well.

MR. CHARROW: Thank you very much, Your Honor. I would like to begin with one overview point. There is apparently some disagreement about the burden of proof that pertains in a case involving a section 1330 case, and I would like to address that to start with because I believe that is an overarching consideration. And obviously, the burden of proof only relates to questions of fact.

And in the context of the Foreign Sovereign Immunities Act, when we're dealing with an exception, it really relates to those facts that are jurisdictional in

nature, that are independent of the facts necessary to establish the textbook version of the cause of action at issue. And in this case there are two such facts.

And also, as an overarching consideration, there are really two burdens of proof. And part of the confusion comes from that. There is the burden of producing evidence. And the burden of producing evidence at this stage of the proceeding rests with the plaintiff. And there is the burden of proof to establish by proof at some point later in the case that the exception to the Sovereign Immunities Act applies, and that would be the defendant's burden.

And the two factual predicates that are independent of the cause of action but are jurisdictional in this case would be, number one, whether the entire tort occurred in the United States, and, number two, was there a personal injury. Those are the two factual predicates that stand as jurisdictional predicates, that are independent of the two causes of action. In other words, these are unusual torts. Both torts can be maintained in textbook format without allegation of proof of personal injury.

THE COURT: My understanding, and I think this is just a version of what you've said, is that the defendant in a Foreign Sovereign Immunities Act case where it is asserting immunity carries the ultimate burden throughout the process.

MR. CHARROW: That's correct.

THE COURT: And that the plaintiff has some burden of coming forward and placing the issue in contest, but that it remains the defendant's burden of ultimate persuasion.

MR. CHARROW: Correct. The ultimate burden of proof rests with the defendant. However, the burden of producing evidence shifts back and forth. And with respect to the burden of producing evidence -- it's a 12(b)(1). Once a plaintiff -- or, once a defendant calls into question the fullness of the pleadings, whether they're adequate, it is then the plaintiff's burden in this context to produce evidence to demonstrate the underlying jurisdictional fact, provided that fact is independent of the textbook version of the cause of action.

THE COURT: This is something perhaps we'll explore more as the arguments proceed, but one question that I'll have -- I can ask you now, but I probably should ask it again when we're closer to the end of the argument -- is whether there is a factual dispute between the parties, or whether it is a legal dispute on these issues. And related to that, if there is a factual dispute, is there any need for jurisdictional discovery in order to decide the pending motion?

MR. CHARROW: It is a dispute based on the pleadings. So it is an 8(a) dispute.

THE COURT: If that's the case, then doesn't the court take the plaintiff's pleadings as true for purposes of resolving the motion?

MR. CHARROW: No, the court does not. Only factual assertions are taken as true.

THE COURT: Fair enough. That's what I meant. But the factual assertions that are in the complaint.

MR. CHARROW: The factual assertions that are in the complaint can be taken as true, if they are in fact factual assertions, as opposed to legal conclusions.

THE COURT: If they are legal conclusions, we don't need facts, the court will decide the law. And if it's a factual dispute, then the court, absent someone putting other evidence before the court, which could occur, that the court would take the pleadings or the plaintiff's complaint as true and any reasonable inferences that can be drawn from the complaint for purposes of deciding the present motion, is that right?

MR. CHARROW: That is partially true, correct.

THE COURT: Tell me where I'm not true.

MR. CHARROW: I think that with respect to the facts as pled, there is a subtle difference between what is sufficient in a normal case and what is sufficient in a 1330 case.

THE COURT: Okay.

MR. CHARROW: And I think there's a heightened standard of pleading in a 1330 case because, unlike in a normal case, you don't have a moving burden of producing evidence at the pleading stage, at the 12(b)(1) stage, and you do in a 1330 case. And that's what's unusual about these cases.

THE COURT: So is there any case that you can point me to saying there's a heightened standard that applies in a 1330 case?

MR. CHARROW: I think any of the Supreme Court cases deal with the fact there's a significant presumption against bringing a foreign country into court in the United States. And it's that underlying presumption that drives the shifting burden of producing evidence. If you look at the, *Chabad* case, for example, it deals with the shifting burden of producing evidence and the fact the pleadings themselves --

THE COURT: I don't understand, though, your emphasis on the shifting burden of producing evidence in a context in which neither you nor the plaintiff is putting any evidence before the court and the court is relying on the complaint. I would understand that if you had come forward with some evidence that might then shift the burden in some way back to the plaintiff to contest that evidence. But in a case in which there's no evidence in front of the

court and there's just a complaint in which the court accepts the allegations, the factual allegations as true, I'm not quite sure I follow the shift.

MR. CHARROW: Let me provide you the context in this case, I think, that makes it clear. I think the one factual allegation that is subject to the moving burden, the shifting burden of producing evidence, is the allegation of mental distress. That is not an allegation that is necessary to establish either cause of action. It is an allegation, however, that is essential to establishing this court's jurisdiction. Without it there is no jurisdiction.

THE COURT: But it's alleged in the complaint.

MR. CHARROW: It is alleged in the complaint, but there are no facts to support it. At the point that we place that at issue, it was the plaintiff's burden to come forward with some evidence or some additional pleading demonstrating that, in fact, an emotional distress in the form of an injury was in fact suffered.

THE COURT: How did you place that issue, that question at issue, other than simply saying we doubt it?

MR. CHARROW: We doubt it -- well, we doubt it in more ways than one. Obviously, it was not in the initial complaint. We pointed that out in our first motion to dismiss. It suddenly appeared as a conclusion in the second complaint, i.e., the first amended complaint.

THE COURT: But not a surprising allegation, given the nature of the underlying allegations in this case.

MR. CHARROW: Not surprising, but when dealing with shifting burdens under the context of 1330 it's incumbent upon the plaintiff to at least present some factual support for the assertion that there is emotional distress. Because, remember, both of these causes of action, when private parties are involved, can survive without a demonstration of personal injury.

THE COURT: Okay.

MR. CHARROW: That's what makes it unusual. Okay? Discretionary function?

THE COURT: Please.

MR. CHARROW: Okay. Assuming -- assuming that the torts exception were to be satisfied with respect to where the tort occurred, the discretionary function exemption obviously must be satisfied in this case. And it obviously exempts from review by a court any activity which is a discretionary function of a foreign nation. And the plaintiff argues that the courts have used, by analogy, the Federal Tort Claims Act. We don't dispute that. We think it provides some analogy. Obviously it provides an analytical basis for which a court can analyze the extent to which a foreign can exercise its discretionary function.

The allegations in the complaint are that there

was spying done. It's not quite clear where the spying was done. It's not quite clear whether the defendant was aware that it was spying on the plaintiff. And I'll get to that shortly. This is all from the pleadings. This is not something I'm making up.

The central point, though, is that a nation, even the United States, has a discretionary function of deciding whether it will spy abroad and on whom it will spy on. And I think we've seen a number of cases where that issue has arisen and the courts have said discretionary function exemption applies here because it's inherent in the decision.

THE COURT: What cases are you referring to?

MR. CHARROW: I think the case involving China, which was, I think, the *Jin* case, State Security. *Jin* versus State Security.

THE COURT: That was a case in which someone was killed, correct?

MR. CHARROW: No, that was not a case in which someone was killed. That's *Liu*. *Liu* was a case where someone was killed. *Liu*, I believe, was out of the Ninth Circuit. *Jin* was, I believe, out of this circuit. And in *Jin* -- that's my recollection. And in *Jin* there was an allegation that Chinese citizens who were adverse to the government were being harassed in the United States by

agents of the Chinese government, and the court said that that's a discretionary function.

Correspondingly, when the head of security of Saudi Arabia was sued for funding, as part of the spying efforts, entities that ultimately were responsible, according to the complaint, in the 911 terrorist attack. Again, the court said that is a discretionary function, who they fund, how they go about their intelligence operations. And, obviously, the plaintiff argues that that type of conduct is not subject to a discretionary function because it's illegal in the United States. Well, obviously, all torts are civil wrongs and the discretionary function exception, obviously, does not apply to all torts.

Let's go back a minute, however. The real question, though, in assessing the discretionary function is whether it is legal or illegal in the country that's performing the actions. And here it's Ethiopia. And under Ethiopia law, it's not illegal to engage in spying overseas. Just as in the United States, it's not illegal for the U.S. government to engage in spying overseas.

THE COURT: That was one of the questions I had, actually. No one actually cites to Ethiopian law in any of the briefing on this issue. What is, in fact, the Ethiopian law with respect to alleged computer intrusions? And, you know, I think you need to be somewhat specific about this

and not simply, you know, simply say, you know, spying, but the question is, is it in fact lawful? And I should say, by the way, I'm taking, for purposes of this entire hearing, the allegations of the complaint as true. I have no idea whether they're true or not.

MR. CHARROW: So are we.

THE COURT: Everything I say, take that, too.

MR. CHARROW: Obviously the defendants disagree with the underlying allegation, but we are accepting as true for the purposes of this hearing only.

THE COURT: Accepting the allegations as true, is there, in fact, Ethiopian law that says that there are individuals in Ethiopia who are authorized, or where it is lawful for people in Ethiopia to reach out through the internet and to intrude into the computers of people in other parts of the world for purposes of eavesdropping on their telephone conversations, their Skype conversations, eavesdropping on what may be going on in their home, reading their text messages? I don't know the answer to know whether that's lawful or not under Ethiopia law.

MR. CHARROW: I believe it is. And I believe it's the same in most nations. Clearly, in the United States the law establishing the CIA gives the CIA the authority to do precisely what Ethiopia is alleged to have done here overseas.

THE COURT: I do think there's sort of an interesting and difficult question I want to spend some time talking about: Illegal in what sense? And you're the one who has said illegal under Ethiopian law. And I think that, you know, under those circumstances, particularly where you're representing the government of Ethiopia, it may your obligation to come forward, if that's what your argument is here, and point me to, hopefully, a translated Ethiopian statute, code, provision, something that says that we are authorized to do this.

I do think that, even putting that aside, that there are some difficult questions about whether that's the right standard of thinking about illegality here. I think you, in your own brief, say that, you know, if an act -- I don't have the language in front of me, but if an act is sufficiently outrageous, that it could rise to the level of -- even if it were not a violation of Ethiopian law, that it is so fundamental it violates international law, that you would say, you know, they're not authorized to do this.

MR. CHARROW: Obviously I don't want to get into a discussion of natural law with the court, but if we're thinking about natural law versus positive law, obviously the cases involving murder would trigger natural law. Fairly uniform recognition that murder is illegal.

THE COURT: One hint of what standard might be

used is in the D.C. circuits opinion in the -- which case was this one? Oh, I guess it was in the *MacArthur Area Citizens Association* case, where the court, in a footnote, says, Well, there may be a difference between crimes that are malium prohibitum and those that are malium in se.

And I guess one question I would have is, is whether, in fact, you know, does one look to U.S. law, does one look to international law, does one look to foreign law for purposes of making this determination? I have some concerns -- I take your point about the analogy to the Foreign Sovereign Immunities -- to the Federal Tort Claims Act, and you might ask whether the Ethiopian official had authority to act as an Ethiopian official, analogous to the U.S. official having authority to act.

I have to say, I think that raises some significant issues about whether it's appropriate and whether Congress would have intended for a U.S. court to be making judgments of that type, which seems to me to perhaps raise even greater comity concerns of reaching into the domestic law of Ethiopia and deciding whether, for example, a particular official in Ethiopia was acting within his or her authority in doing something, at least raises some issues that I think ought to make a U.S. court a little bit uncomfortable and question whether that's the right standard.

Similarly, one might say that as a U.S. court, you

know, I ought not say someone has discretion to violate the law in this country. And I take your point about negligence and things like that, but maybe that's where you get into the malium prohibitum and malium in se or, as the Restatement does, the difference between serious crimes and nonserious crimes.

But there is something -- and the cases don't speak terribly directly to any of this, but there's something a little bit troubling about a U.S. court saying, Oh, yeah, someone was acting within their discretion when they came into the United States and committed a clear violation, and I'm not saying that's this case, but a clear violation of U.S. law in some way.

In the *Letelier* case -- I mean, you know, I'm not sure you need to turn to international law or the law of humanity to simply say that it's troublesome for a U.S. court to say that someone was acting within their discretion to come into the United States and in the United States assassinate somebody.

MR. CHARROW: Correct. And that's why, I think, I was talking about natural law and the concept of those types of actions that are universally viewed as reprehensible.

THE COURT: So let me get at that. How would you articulate that standard? If the standard is not just the law of Ethiopia, but there's, you know, a second prong to

it, it's -- you know, even if they had authority under Ethiopian law, if they did something that was X --

MR. CHARROW: I think most courts that have addressed this issue have either overtly or subconsciously reverted to U.S. law. And they have said, okay, make believe this were the U.S. government acting overseas. Would this be legal or illegal under U.S. law? Would this be viewed as a discretionary function of U.S. law if it were done overseas? And this type of conduct here, as alleged in the complaint, clearly would be within the scope of what the CIA is expressly authorized to do by statute.

So if you use the U.S. law as a gloss, if you will, as a template for what is proper and what is not proper in terms of discretionary function, I think you come away with the understanding that this would be a valid exercise of a nation's discretionary function.

THE COURT: How would you articulate the standard though?

MR. CHARROW: I think I would look at it as a two-prong standard. First of all, I would ask myself, Is this something that is so inconsistent with universal norms as to be condemned by all nations? A standard very similar to that which would be used in the international legal area.

The next question would be if it isn't, then is this a type of activity which, if done by the United States

abroad, would in fact be viewed as something subject to governmental discretion? And I think in both cases we find that this is not something that would be viewed as reprehensible internationally and, number two, it is something that is done by the United States abroad and pursuant to its discretion. And if you apply that to this case, I think it would be -- I think it would be inappropriate for a court to say, well, the United States can do it overseas, but another nation can't do it here, in terms of exercising its discretion in its homeland, making a decision what to do.

THE COURT: Well, that actually raises another question which has been on my mind, which is has anyone actually asked the United States what their position is with respect to this case? Has anyone raised the question with the United States as to whether the United States should file a statement of interest?

MR. CHARROW: Normally the State Department, in my experience, does not file statements of interest, normally, in District Court proceedings. They wait until a matter pops up to Court of Appeals.

THE COURT: Do you know whether it's been raised with the State Department at this point?

MR. CHARROW: I can't say one way or another.

THE COURT: Any views on whether the court should

ask for the State Department's views? Frankly, as a District Court Judge I don't -- it's not the best --

MR. CHARROW: I guess the issue is this: The issue is -- there are a lot of issues in this case, for example, that arguably raise potential Constitutional issues. This court can dispose of this case without getting to those issues.

THE COURT: So there's another line of defenses in this case, I take it, that if these defenses fail, is there an active state defense?

MR. CHARROW: We haven't raised an active state defense, Your Honor. I think that the Federal Tort Claims Act, tortious exception 1605(a)(5) in this Circuit and in the Ninth Circuit and in the Second Circuit and in the Sixth Circuit require that the entire tort be committed in this country.

THE COURT: That will be our next segment.

MR. CHARROW: And that hasn't occurred here. And that, to me, is the cleanest and easiest way to resolve this case.

THE COURT: Is the reason you raise that point now is because the Active State Doctrine usually applies to conduct that occurs outside the United States?

MR. CHARROW: Correct.

THE COURT: Are there other Constitutional

defenses?

MR. CHARROW: There are Constitutional issues. There is one lurking that's very subtle, that we did not raise in our briefs, but it is there nonetheless, and that's the definition of person.

THE COURT: You did raise that in your briefs.

MR. CHARROW: We did, but I don't believe we raised the Constitutional issue in the brief, to alert the court that if it were to hold that the word "person" included a foreign entity, then one has to look back and question whether the in persona jurisdictional provisions are Constitutional of 1330.

Because, remember, in this Circuit a foreign state is not a person for due process clause protections. That permits service of a foreign state in the United States, even though it doesn't satisfy minimum contacts. If a foreign state is a person, then we have a Constitutional issue of due process.

THE COURT: I see your point. Did service occur through the State Department in this case?

MR. CHARROW: I don't know how service was perfected in this case. We received it after the fact and --

THE COURT: Would you have any objection to the court asking if the United States cared to express its views?

MR. CHARROW: We do not. We would not object to

that, Your Honor.

THE COURT: Okay. Another question with respect to the discretionary function exception is -- there's no briefing on international law. And I guess I had a question about whether you have a view as to the type of conduct that is alleged here, whether it's consistent with international law, whether it's consistent with the international covenant on privacy and civil rights to which, I believe, Ethiopia is a signatory -- or, not a signatory, it's a party.

MR. CHARROW: I believe it's consistent with international mores, which I think is more important in that respect.

THE COURT: Well, but is it consistent with international law or not?

MR. CHARROW: I believe the actions are consistent with international law.

THE COURT: What about the international covenant on privacy and civil rights?

MR. CHARROW: I believe that the actions here would be consistent with that.

THE COURT: Any view about whether the conduct at issue that is alleged here is malium in se or malium prohibitum?

MR. CHARROW: Haven't thought about it long enough to give you an answer. I just view it very simply as

something that falls well outside the area that would not be subject to a discretionary function exemption.

THE COURT: All right. Anything further on discretionary function?

MR. CHARROW: I think not.

THE COURT: Let me hear from the plaintiffs then.

MR. CARDOZO: Good afternoon, Your Honor. Thank you.

THE COURT: Good afternoon.

MR. CARDOZO: As my opposing counsel did, I'll start with just a very brief introduction about why we're here.

Congress has, of course, given foreign governments wide berth and immunized them against civil actions for many torts. But, the question before this Court is whether a foreign sovereign has discretion to commit a violation of the Wiretap Act, which is a tort as well as a serious felony, discretion that not even the U.S. government claims for itself. So -- and I will, if Your Honor will allow it, switch to burden very briefly. Or would Your Honor prefer I go to straight to discretionary function?

THE COURT: I was thinking about what you said in your opening. Let me get that up a second.

MR. CARDOZO: Yeah, I will.

THE COURT: Feel free to go to burden.

MR. CARDOZO: I'll continue on discretionary function, actually. As a court in this District ruled in *Orlikow* versus United States, that court found that CIA agents have no discretion to commit intelligence operations that are lacking in statutory authority. That's the case that controls here. You know, if a CIA agent was caught here in the United States and violated the FTCA. Same thing would apply to an Ethiopian agent if they were caught here.

CIA agents, when they conduct intelligence operations undercover abroad, if they get caught, they go to jail. It's not something that is legal for CIA agents to do. That's essentially what the government in Ethiopia is claiming here, that what CIA agents can't do, or if they did do they would get sent to jail, that Ethiopia can.

The question that this Court asks in determining whether the spying alleged here was a discretionary function is whether this is the type of judgment that Congress meant to immunize. And the Foreign Tort Claims Act case law cited in *Letelier* shows that this is not the type of judgment that Congress meant to immunize. This court, in *Letelier*, stated that foreign states have no discretion to have their officers commit an illegal act. Of course, illegal acts must be sufficiently grave to fall outside the discretionary act exception.

And *Orlikow* shows us that violating a federal

criminal statute for which, here, a Wiretap Act violation, carries a five years prison sentence. There's no discretion.

THE COURT: Is that true for the Federal Tort Claims Act as well? If there's some level of seriousness -- seriousness threshold that has to be met before an act is deemed to be nondiscretionary?

MR. CARDOZO: So in the Federal Tort Claims Act, as in the Federal Sovereign Immunities Act, there's a two-step process. The first is, is there an element of choice? And that's where defendant fails. If U.S. criminal law prohibits one of your options, with a serious enough -- and there is no bright line, there's no -- "serious enough" is not a bright line distinction. But if U.S. criminal law prohibits one of the options but offers a regulated lawful pathway to go about accomplishing the same end, then there's no discretion to go about the illegal channel.

And here there is a mandatory channel. Ethiopia could have accomplished this act of spying in the United States legally if it had wanted to. We have a mutual legal assistance treaty framework. Ethiopia is not a signatory to an MLAT with the United States. But even if it's not a signatory to an MLAT, it still may request State Department or Justice Department assistance collecting evidence. And that happens all the time, Your Honor.

THE COURT: Is the allegation here that Ethiopia

was engaged in a criminal enterprise or an intelligence enterprise? And if it was intelligence versus criminal, is there any authority or basis for seeking mutual assistance in an intelligence activity?

MR. CARDOZO: Your Honor, the plaintiff is not aware whether this was considered a criminal or an intelligence operation. And there's no distinction, Your Honor. At the MLAT framework there is no distinction whatsoever. And at least in this Circuit the defendant is simply wrong. This court, in *Letelier*, said that we look to U.S. law to determine whether a discretionary function is being exercised.

THE COURT: It went a little bit beyond the U.S. law and talked about crimes against humanity or something to that effect. There was some language in there which was stronger than just this was a violation of U.S. law. And I assume it was also a violation of Chilean law as well, I would assume.

MR. CARDOZO: That is certainly possible, Your Honor. And notably, the defendant hasn't alleged that they, for instance, got a warrant to serve on Mr. Kidane. But in any case, the conduct that happened here was not consistent with the international covenant on civil and political rights. The -- that covenant requires that intelligence activities or surveillance be necessary and proportionate.

And defendant has not made even an argument, much less a showing, that the -- this surveillance was necessary and proportionate.

THE COURT: Can I ask you another question about the International Covenant, which is, based on my reading of it, it -- let's see if I have it here. It's Article 17 says, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence." Is that the provision you're relying on, as well?

MR. CARDOZO: Yes, Your Honor.

THE COURT: When it refers to unlawful interference, this gets us back to the same question again: Unlawful under international law, unlawful under the law, the domestic law of the target nation, or unlawful under the domestic law of the targeting nation?

MR. CARDOZO: I think in the covenant, Your Honor, that it's referring to international law. But here we can look to U.S. domestic law and international norms, as did the court in *Letelier*, as do courts in this Circuit generally.

THE COURT: But the International Covenant, in particular Article 17, is not self-executing in the United States.

MR. CARDOZO: That's correct, Your Honor. And we

have the Wiretap Act to do that work for us here.

THE COURT: So what work does the International Covenant do for you?

MR. CARDOZO: It's just simply another indication that the conduct that Ethiopia subjected Mr. Kidane to is simply not accepted at international law or at U.S. law.

The other case, which is a Foreign Tort Claims Act, which I think speaks directly to this, is from the district of Hawaii, which is *Cruikshank versus United States*. And in that case CIA agents were found to not have the discretion to break the law in the course of an intelligence operation. *Cruikshank* is also important because it shows that privacy torts are not barred by the -- in that case the FTCA, and this is, of course, a privacy court.

And then --

THE COURT: How would you articulate the test, the test for unlawfulness?

MR. CARDOZO: The test for unlawfulness, Your Honor, is was there an element of choice? Here a federal felony criminal statute takes away the element of choice. And second, was there a mandatory pathway? And again, the answer is yes.

THE COURT: On prong one, how do you distinguish the *MacArthur Area* case then?

MR. CARDOZO: Your Honor --

THE COURT: We know there isn't a choice to violate the zoning laws.

MR. CARDOZO: Indeed, Your Honor. But it wasn't a felony. No one was going to jail for five years for violating a zoning law. Similarly, in the consular assistance cases, no one is going to jail for those. In a grant recommendation, no one is going to jail.

THE COURT: So it turns on the seriousness of the crime?

MR. CARDOZO: Indeed, Your Honor.

THE COURT: Here you said that it's a felony. And it struck me, on reading the briefs, that you have an argument, and a substantial argument, that a foreign entity may be subject to civil suit under 2520.

MR. CARDOZO: Yes, Your Honor.

THE COURT: Because that statute refers to person or entity. But the criminal provisions of the statute refer to just persons. And so do you actually have an argument here that anything Ethiopia would have done would have been criminal?

MR. CARDOZO: Your Honor, if I was a U.S. attorney standing up here with the Ethiopian intelligence agent who directed this operation in the witness box, perhaps I would.

THE COURT: But with the individual, not the

nation then?

MR. CARDOZO: Correct. But, obviously, I'm not a U.S. attorney.

THE COURT: Right.

MR. CARDOZO: Turning to the issue of burden here, the motion to dismiss --

THE COURT: To be clear, I don't mean to be suggesting that there -- you know, that I have reason to conclude there's anything criminal here. As I said, I'm just taking the allegations as started in your arguments as stated.

MR. CARDOZO: Yes, Your Honor. Turning to the issue of burden. As opposing counsel noted, it is -- it's not particularly straightforward, but it's not as complex as opposing counsel suggests. At the motion to dismiss phase, Ethiopia has its initial burden to show that it is in fact a foreign sovereign and entitled to immunity. And, of course, it has met that burden. The burden then shifts to the plaintiff. And at this stage, at the motion to dismiss stage, all that's required is that the plaintiff assert allegations sufficient to bring this claim within the exception. And that comes directly from *O'Bryan versus Holy See* out of the Sixth Circuit.

And our evidence here is that there's been an interception; that Mr. Kidane's Skype calls, his web search

history, possibly his e-mail as well, and that of his family, were all monitored by the government in Ethiopia. And that's all that's required to get past a motion to dismiss.

THE COURT: Let me ask you another question about the discretionary function exception here. I take your point, there certainly is lots and lots of support in the case law for modeling the discretionary exception, kind of discretionary function exception under the Foreign Sovereign Immunities Act and the Federal Torts Claims Act, it was modeled on it in the cases cited. But they don't apply in exactly analogous circumstances. And the purposes of the Federal Tort Claims Act and the Foreign Sovereign Immunities Act are not the same.

And going back to John Marshall, one of the principal reasons for having foreign sovereign immunity is comity between nations. And if I were to rule your way on this case, does that open the door to a situation that, not necessarily in this case or just in this case, but more broadly gives rise to pretty serious foreign policy issues where -- and, again, let me not use this case because I don't want to comment, necessarily, on this case in any way, but imagine a case in which someone has a grudge with a nation that they've left and they left on bad terms, there's some hostility between somebody who's moved to the United

States from that nation. The person comes into court and says, You know what? I think I've got a good enough basis to believe, you know what? there's guys back in my old country, I think they're spying on me.

You come in, maybe there's a little bit of evidence on that, and someone comes in and says, Okay, now I want to subpoena the head of intelligence, you know, the prime minister, I want to find out if it was authorized. You know, I got to ask the prime minister if the prime minister authorized this. I have to delve into, you know, highly confidential either law enforcement or intelligence activities of a foreign nation and have this federal court doing that. Doesn't that raise the sort of comity concerns that animated the Foreign Sovereign Immunities Act and foreign sovereign immunity going back to the beginning of the nation?

MR. CARDOZO: It might, Your Honor, but, luckily, that's not the case we have in front of us and that's not the case that this Court is going to face going forward. In FSIA context, discovery -- factual discovery is not permitted until after a motion to dismiss. And just stepping back a little bit further, the Mutual Legal Assistance Treaty framework, which the U.S. is a vibrant participant in, would be rendered superfluous if the Ethiopia government's argument was correct. What Ethiopia

has argued to Your Honor today is that their failure to sign a Mutual Legal Assistance Treaty with the United States gives them more power than if they had.

THE COURT: My point, though, is the legal principle that you're arguing for here -- again, putting the facts of this case aside, or the allegations in this case aside, but the legal principle is that if someone from outside the United States, a foreign state reaches into the United States in a way in which someone can make an allegation that they've committed a felony, that that then allows a federal court to take jurisdiction over that matter in a way that could, at least in some cases, really upset a fairly delicate set of issues of foreign relations.

You could imagine a case in which a judge -- again, not this case, but you can imagine a judge, based on that type of policy, the use of the subpoena power and so forth, could strain, if not worsen relations with a foreign power. Could, where you -- could have had, you know, the United States government could have been working very carefully -- again, not this case, but could have been working very carefully to establish some sort of relationship with a country, could have gotten very close to, you know, a treaty of some type with the country, could have been huge U.S. interests in this issue, and all of a sudden you've got a judge who's dragging in the head of

intelligence saying, you know, I need to know what happened here and let's do some depositions. And the foreign government starts saying, you know, this is out of control and, you know, is calling up and yelling at the president about this crazy judge.

And I'm really more getting at the principle here than the particular facts of this case. And how do you draw the line in a way to make sure that that purpose of the Foreign Sovereign Immunities Act isn't overridden by whatever rule you're asking me to adopt?

MR. CARDOZO: Two points in response, Your Honor. First, federal discovery does not extend, I think, to the extent that Your Honor is worried about. If a U.S. litigant attempted to haul the chancellor of Germany into a deposition, a federal court should and would grant a protective order to stop that. So that's not what's going to happen.

The second thing is the diplomatic harm or the nation-to-nation harm that occurs is simply the harm that occurs when spies get caught. That's just when spies -- when a spy of a friendly nation or of a not-so-friendly nation gets caught, diplomatic harm occurs.

THE COURT: There may be a difference in whether the authorities in one of those nations is making a decision about whether to prosecute that person versus, you know,

allowing a civil litigant and a nonelected judge to make the decisions about whether to create what could become an international crisis.

MR. CARDOZO: Perhaps, Your Honor. But Congress gave this court, with the Discretionary Act exception, gave this Court the power to decide whether this is the sort of tort that was intended to come within this Court's power. And here the answer is yes.

THE COURT: Is there some other doctrine that would address the types of concerns that I'm raising, so that even if the court were to conclude that it had jurisdiction over the matter, that there might be, if not active state, which I guess is also in the form of immunity, but, you know, they're -- for example, there are cases that preclude state courts, like the *Garamendi* case and those lines of cases, from adjudicating matters where doing so could interfere with foreign relations? Is there some other doctrine that would provide a safety valve for the types of concerns I'm talking about?

MR. CARDOZO: First of all, the Active State Doctrine can't apply because it only applies to conduct within the territory of the foreign state. So that's not at issue here. The Political Question Doctrine might apply, but no court has ever applied it in the Foreign Sovereign Immunities Act context.

THE COURT: What about the assertion of the foreign relations powers, the separation of powers issue?

MR. CARDOZO: There is no such doctrine, at least not to dismiss an FSIA case. No federal court, to my knowledge at least, has applied such a doctrine in the FSIA context. And Congress didn't intend that. Congress intended that for nondiscretionary acts that create personal injury here in the United States, and acts that occurred here in the United States, that this court should exercise its jurisdiction. This court has jurisdiction to hold the foreign sovereign accountable to that.

Something my opposing counsel said, the privacy torts that we've alleged here are per se personal injury and nothing further is required. And that comes -- that comes from *Pearce versus E.F. Hutton* out of this District. Both intrusion upon seclusion and the sort of interception that we've alleged that's a violation of the Wiretap Act are per se a personal injury. And in terms of the burden of producing evidence, that's all that's necessary at the motion to dismiss phase.

Opposing counsel has cited no authority to say that the plaintiff needs to produce anything other than an allegation that what has happened is, by definition, personal injury.

THE COURT: The hypotheticals that I was throwing

at you a minute ago, which admittedly, you know, are not this case, but go to the question of how to articulate a rule here, involve the equities of the executive branch and perhaps the legislative branch. Do you have a view on whether this court should at least provide the government with an opportunity to be heard on these issues? Do you know whether anyone has explored that issue with the government thus far in the litigation?

MR. CARDOZO: We have not, Your Honor. And while we have no objection to the Court reaching out to the Department of State to get its views, we don't think it's necessary. Certainly the motion to dismiss phase it's not necessary.

And then if Your Honor has no further questions on the burden or on discretionary functioning.

THE COURT: Why don't we move on to the entire tort. Okay. I'll hear from the defendant.

MR. CHARROW: Thank you, Your Honor. Since 1984 the law in this Circuit has been fairly straightforward. The entire tort has to occur in the United States in order for the exception to be triggered. And that's largely an outgrowth of the legislative history, the language of the provision, Supreme Court opinions prior to 1984 and thereafter, and a string of cases that has consistently held that the entire tort must occur in the United States. And

there's good reason for that. And there are a lot of policy reasons why we would want the entire tort to occur in the United States, as opposed to piecemeal, some here, some there. And I can go through those one by one with the court, if the court would like.

THE COURT: Sure. Whatever you think is helpful.

MR. CHARROW: I think some of these would be helpful. I think, first of all, we have a general presumption against extraterritoriality. And if we look, for example, at -- if we compare, for example, 1605(a)(2), which is the commercial exception to the Federal Tort Claims Act, with 1605(a)(5), which is the tort exception, which is the one before the court today, you'll note that (a)(2) does permit activity to occur overseas. It expressly so permits. Those express terms are not present in 1605(a)(5).

So quite aside from the law of the circuit, we have general notions of statutory interpretation, coupled with the concept of a presumption against extraterritoriality. The statute itself was primarily designed to enable citizens in the United States to sue for auto accidents. And auto accidents, by definition, occur entirely in the United States.

If we look at a number of the cases that were cited -- now, plaintiff argues that a lot of the cases that were cited are cases where things occurred overseas. Well,

that's the point. When things occur overseas, people frequently attempt to sue in the United States. And a number of cases, though, involve what I call split torts, where some of it occurred there and some of it occurred here. And the courts have consistently held in those cases that there's no cause of action.

I think the Colorado aircraft case, *Four Corners*, was a products liability suit against the French engine manufacturer that was owned by the French government. The crash occurred in Colorado. A portion of the tort occurred in the state of Colorado. And the Court said 1605(a)(5) did not trigger because the entire tort did not occur in the United States.

THE COURT: My recollection was it was actually something -- was it in Mexico that it actually occurred, where it was some sort of -- I can't remember if it was a supervision or some negligence that actually occurred in Mexico, as well.

MR. CHARROW: Could be. And I think the courts have consistently so held. I don't know of any court that has held that a tort that is committed overseas can give rise to a federal -- to an exception provision, trigger the exception provision of 1605(a)(5).

THE COURT: So you were certainly right, that there is precedent from the Circuit here that says that the

entire tort has to occur in the United States. I guess the question for me is what that means. And most recently, the Court of Appeals in a case called *Jerez versus Cuba*, described it this way, they said, "The law is clear that the entire tort, including not only the injury, but also the act precipitating that injury, must occur in the United States."

And then it went on and distinguished the situation and said, "Jerez seeks to reinforce the parties' redeployment analysis by analogizing the defendant's actions to a foreign agency's delivery into the United States of an anthrax package or a bomb. But here the defendant's infliction of an injury on Jerez occurred entirely in Cuba." He was, I believe, infected with hepatitis C. "Whereas, the infliction of the injury by the hypothetical anthrax package or bomb would occur entirely in the United States."

And it sounds to me like what the court is saying there is that when it refers to the entire tort occurring in the United States, it requires two things: One is that the injury be in the United States and, two, that the act that precipitated that injury occur in the United States. But I take it that that's what the plaintiffs are alleging here, at least, it did in fact take place.

MR. CHARROW: I think you have to step back. What does the tort consist of? These are both intentional torts. They require the marriage of mens rea, or whatever the state

of mind necessary for an intentional tort is, and the act itself. The two have to coexist. Here there is no doubt and no dispute that all human behavior occurred in Ethiopia. There is no allegation that any Ethiopian agent of the government of Ethiopia was present in the United States.

What is surprising is that if we step back a moment and look at the original infection, the original computer virus -- remember, the plaintiff here was not the target of that virus. The plaintiff's friend was. Where did that occur? That occurred, finally I figured it out, occurred in London. If you look at the translated version of Exhibit C, it appears that the individual who was originally infected was residing in London. And there's no allegation that that person was present in the United States in this complaint.

So the actual act did not even occur here. So I find it very difficult to understand how any part of the tort occurred in the United States. Certainly all of the acts occurred overseas. The actual reading of the documents, to the extent they occurred overseas, the intent was developed overseas, the service was located overseas, all of the individuals were overseas. Nothing occurred here.

THE COURT: I will, obviously, let the plaintiffs address that. But let me at least try what I think they

might say, just to get your response to it while you're standing here, which is -- I take it from reading their papers what they would say is that when the invasive code ended up on someone's computer in the state of Maryland, that someone then still had to activate that in some way. They may have activated it from Ethiopia, but the result of what they did was to turn on, in essence, a tape recorder on someone's computer sitting in Maryland.

And by, sort of, by analogy, maybe a circumstance in which, you know, I'm on vacation in Canada and I pick up the telephone and I call a friend of mine and I say, hey, there's a tape recorder under the desk in someone's office, can you do me a favor and go and flip it on? That person has no mens rea because they -- they don't know what they're doing, they're just staff and they turn on a tape recorder. But, in fact, that is -- was an illegal recording that was taking place purely in the United States and that was the act that precipitated the injury, was that recording. And so I'll hear from the plaintiffs, but I take it that's what their theory is in response to it.

MR. CHARROW: Right. They're arguing, basically, that a robot can commit a tort. The Restatement Third has not reached that point yet. The Restatement Third --

THE COURT: We live in a word in which the internet is pretty expansive.

MR. CHARROW: I recognize that. And as courts have recognized frequently, the law does not keep up with the internet. But in this case we are requiring the entire tort, including the intent, to be developed in the United States. That is the law of this Circuit.

THE COURT: And is there any case that actually says you need the intent in the United States? That's where I'm pausing a little bit, particularly this case that I just mentioned to you, because it doesn't say anything about the intent. It suggests that if someone were to mail a package into the United States that contained a bomb or anthrax, that that might be sufficient. It's dicta in the decision. But it's dicta from the Court of Appeals here. It seems that might be sufficient.

MR. CHARROW: The cases that we've seen do in fact have intents developed overseas with effects in the United States and the courts have held that's just insufficient.

THE COURT: Well, but there's usually something else that's taking place overseas in the cases that I've read. If there are cases where the only thing that occurs overseas is the intent, you ought to point me to them.

MR. CHARROW: I think the closest is the Mexican case from 1984.

THE COURT: The case we were talking about before?

MR. CHARROW: Correct.

THE COURT: I believe, and I need to go back and look at that myself, my belief is that the court held that the problem was that there was either some negligent supervision or some negligence that occurred.

MR. CHARROW: We're talking about a different case. We're talking about the 1984 case. My pronunciation is abysmal, it's --

THE COURT: You can spell it.

MR. CHARROW: It's *Asociacion de Reclamantes*.

THE COURT: Oh, yes.

MR. CHARROW: Scalia decision.

THE COURT: Okay.

MR. CHARROW: From '94.

THE COURT: *Reclamantes*, I believe.

MR. CHARROW: Right. And in that case the court was having difficulty figuring out precisely what the tort was. Because it was unclear whether the tort was the original taking of the property or was it the subsequent refusal of the state of Mexico to recompense the family for the taking of the property.

THE COURT: Right. But what the court actually held in *Reclamantes* was the tort occurred exclusively in Mexico.

MR. CHARROW: No, it didn't.

THE COURT: I believe it did.

MR. CHARROW: It did not hold that. It stated the entire tort has to occur in the United States. But a portion of the tort, to the extent that there was an injury, that occurred in the United States because --

THE COURT: Maybe -- the injury may have occurred in the United States, but my recollection of what the court held was is that by that point in the litigation, it was a complicated history, but what happened was that there was a dispute with respect to land, it was settled between the United States and Mexico.

MR. CHARROW: Correct.

THE COURT: Individuals in the United States originally had claims against the U.S. government for taking their land. The Mexican government agreed to take on that responsibility and said we will pay them for the land. Took on that responsibility pursuant to a treaty or agreement with the United States, and then didn't pay.

MR. CHARROW: Exactly.

THE COURT: And what the Court held in *Reclamantes*, I believe, was that the tort that occurred was the omission by the government of Mexico, city in Mexico to pay the amount that they were required to pay.

MR. CHARROW: Arguably, with the failure to send a check in to the United States.

THE COURT: Well --

MR. CHARROW: It can be viewed either way. It was cross-border activity, is the bottom line.

THE COURT: Right. But what I was asking you, though, is whether -- was there any case that says that where the only element of the tort that did not occur in the United States --

MR. CHARROW: Was the injury?

THE COURT: No, with the formation of the required mental state, the intent.

MR. CHARROW: I can't think -- I can think of none. But, of course, here none of the human acts occurred in the United States. So it was not just the intent, we're talking about the human acts.

THE COURT: But what about this hypothetical, thought, from the *Jerez* case where the court says, you know -- suggests, at least, that it might well be sufficient if someone were to mail a package into the United States that contains anthrax or a bomb. There, you know, no tort feasor is in the United States, but the tort is taking place in the United States and the injury is occurring in the United States.

MR. CHARROW: It's like throwing a bomb, if you will, from the Canadian border into the United States. Part of the act occurred in Mexico -- in Canada, part in the United States. That's the hypothetical.

THE COURT: Yeah. I mean, you know, as I say, I don't think it's a holding, I think it's dicta from the court.

MR. CHARROW: But I don't think that any court has ever addressed -- has retreated from the entire tort view when faced with the actual set of facts.

THE COURT: But let me put it this way: You, a minute ago, said that one of the rationales for the entire tort doctrine was that there's a general presumption against extraterritoriality. I would have assumed that the presumption against extraterritoriality would not apply where, in fact, the action that gives rise to the injury occurs in the United States, even if the intent was formed outside the United States.

So you have, for example, you know, in an antitrust case, you've got people outside the United States -- and I can't, frankly, remember off the top of my head, remember if the Sherman Act applies extraterritorially or not, but assume it doesn't for purposes of this. You have people outside the United States who decide where to engage in price fixing in the United States, they get on the telephone and call all of their vendors in the United States and say set the price at X dollars and, as a result of it, every vendor selling a particular good in the United States is selling it at a particular price. Maybe the people with

the specific intent are outside the United States, but the tort is arguably -- I wouldn't think the ban on extraterritoriality would apply.

MR. CHARROW: Let's look at OPEC, it's a good example. The antitrust example you gave is a great example. If the tort exemption did not apply, citizens of California could sue under 17200, the Business and Professions Code.

THE COURT: I don't know the story with respect to OPEC. I assume someone might assert the commercial exception, which does apply outside --

MR. CHARROW: Let's make believe that I allege a tort, and I certainly can construct a tort out of price fixing and market shares, can I not, and of allocation of markets.

THE COURT: Okay.

MR. CHARROW: Okay. And if I can do that, I can sue under California's Cartwright Act, I can sue under California 17200.

THE COURT: Are there any cases that deal with this issue?

MR. CHARROW: The point is there are none, and there are none for a reason. Because what occurs outside the United States, is not subject to 1605(a)(5). That's why no one has sued, even though there's a pot of money there.

THE COURT: That may be a circumstance -- I'm not

familiar enough with it, though. May be a circumstance in which the injury is just occurring in the United States, but where the actual sale is taking place outside of the United States. I don't know the answer to that question.

MR. CHARROW: The sales are occurring here, actually. When you stop and think about it, you're buying the gasoline, the crude oil is coming into the United States.

THE COURT: I meant the sale from the --

MR. CHARROW: Sales come directly from those nations to the United States. So part of the tort occurs here, the injury occurs here, the mens rea occurs there, the conspiracy occurs there.

THE COURT: Are there cases that hold that the entire tort rule bars an action against OPEC?

MR. CHARROW: There was a case that did not get resolved, in 1982, that I was involved in, which was the Westinghouse antitrust litigation, where this issue was raised but the case was settled before court was involved. But it certainly involved price fixing of uranium by foreign nations.

THE COURT: Anything more on the entire tort issue?

MR. CHARROW: I think we've exhausted it. I think it's well briefed by both parties.

THE COURT: Let me ask you, our conversation was

proceeding on the assumption that the only element from outside the United States was the specific intent. Is that your position or --

MR. CHARROW: No, no.

THE COURT: Part of it, I think, is the question of how you define the tort. I want to give you a chance to do that.

MR. CHARROW: Here all of the acts occurred, all the human acts occurred outside the United States. No human act occurred in the United States.

THE COURT: Where do you think the interception occurred?

MR. CHARROW: There was no interception under the Wiretap Act. Zero.

THE COURT: Was there any interception anywhere?

MR. CHARROW: There was no interception. But they're relying on the Wiretap Act. There was no interception under the Wiretap Act.

THE COURT: Would the Stored Communications Act provide a cause of action then?

MR. CHARROW: No, it would not.

THE COURT: The Computer Fraud and Abuse Act?

MR. CHARROW: Don't know. But I certainly know that the Act that they're relying on, which is 2511 and 2520, provides no cause of action here.

THE COURT: What about their argument that the interception was, in essence, turning the plaintiff's computer into their own tape recorder?

MR. CHARROW: I think they recognize that the Wiretap Act, as have a number of cases, that the Wiretap Act was passed many, many years before the internet. And if they want to use the Wiretap Act to address this case when it doesn't, Congress is going to have to amend the Wiretap Act accordingly.

THE COURT: It was amended in 1986.

MR. CHARROW: I'm talking about post internet. The internet as we know it really didn't come into existence until the '90s. It was crude e-mail before.

THE COURT: Okay. Anything further on this issue?

MR. CHARROW: I assume I'll come back to the Wiretap Act.

THE COURT: Yes, yes.

MR. CHARROW: Okay.

THE COURT: All right. Let me just pause for a second here, ask the court reporter when you would like to take a break.

You're okay? After this. Why don't we go through this segment and then we'll take a break.

MR. CARDOZO: Thank you, Your Honor. And I appreciate your patience with what is turning out to be a

long argument.

Before I start on location of the tort, let me clarify two points that I made earlier. The first is that entities, in fact, can commit crimes through their agents under 2511; it's just that the entities can't be prosecuted, only their agents can.

And then second, we haven't asked the State Department specifically for their views. I wanted to just be clear that it was the State Department that we did not ask.

THE COURT: Okay.

MR. CARDOZO: The invasion of Mr. Kidane's privacy occurred in his home in Silver Spring, Maryland, and not anywhere else. And *United States versus Rodriguez* out of the Second Circuit tells us that the interception occurs where the conversation was happening. In *Rodriguez* it was a telephone. In *Rodriguez* the court said the interception occurred at or very close to the telephone itself. And that's what we have here. The interception at or very close to Mr. Kidane's home.

THE COURT: I thought that the relevant law on this was the interception occurs in two places, at least with respect to the Wiretap Act more generally. It occurs, you know, using old style versions of -- thinking about this, where the alligator clips go on the line and where the

listening post is. Is that not --

MR. CARDOZO: That's actually not the law, Your Honor. The interception occurs when the acquisition is made. And where, or even if it was listened to is irrelevant for that purpose.

THE COURT: Right. But the cases I'm referring to are the older cases that dealt with the court's jurisdiction to enter -- or, to authorize an interception. I thought that's what they said. But the point is where the clips go on the line, the alligator clips in the old technology, is where the interception would occur.

MR. CARDOZO: Exactly, Your Honor.

THE COURT: And here, I take it, your position is that, as I was saying to your colleague, that the interception, in essence, was the commandeering of the plaintiff's computer and using the plaintiff's computer to make a recording for the defendant. Is that your position?

MR. CARDOZO: It is, Your Honor. And more specifically, it's the creation of the additional files on Mr. Kidane's computer. So it's not just the commandeering of the computer, it's not just the potential to listen to, it's the fact that his Skype calls were actually copied by the FinFisher software and saved on his computer in Maryland.

THE COURT: I understand that point conceptually. Are there any cases that have ever embraced that theory?

MR. CARDOZO: You know, this is the first case where we've seen a -- this particular type of malware under the Wiretap Act. It almost certainly won't be the last.

Something that opposing counsel said was that he was aware of no cases where the intent was formed, the tortious intent was formed abroad, but yet courts found. *O'Bryan versus Holy See* is that case, Your Honor, out of the Sixth Circuit. There there were several causes of action. The Sixth Circuit dismissed some but allowed others to proceed. The ones they dismissed were the ones that occurred entirely outside of the United States; namely, the negligent training and supervision of the priests. But the cause of action that *O'Bryan* allowed to proceed was the application of policies that were formed in the Vatican in the United States.

And that's what we have here. We have the application of policy formed in Ethiopia, the intent to wiretap Mr. Kidane, its application in the United States, the actual wiretapping of Mr. Kidane succeeds, and that's where the tort happened.

Just like in *Jerez versus Cuba*, this is the digital equivalent of the anthrax packet mailed into the United States. There's no conceptual difference here. It's just one happens on the internet and the other happened --

THE COURT: Do you agree that that language in

Jerez is dicta though?

MR. CARDOZO: It is, Your Honor. But it's instructive and it should guide this court's reasoning. And the logic is, frankly, persuasive.

In the Computer Fraud and Abuse Act context courts apply this quite regularly. In the *United States versus Ivanov*, for instance, there was a Russian hacker hacking entirely from Russia, compromising computers in the United States, and that posed no bar whatsoever. The crime was committed here, where the computers were, not where the criminal happened to be. And that's noted right here.

What matters is where the relevant conduct occurred. Here the relevant conduct is the interception, the acquisition of Mr. Kidane's phone calls. And for the intrusion upon seclusion tort, the monitoring of his web searches and e-mail. All of that happened at his home in Maryland.

THE COURT: One question about the Maryland state common law claim, if the court finds that there's a waiver of immunity under the Foreign Sovereign Immunities Act with respect to the wiretap claim, is that sufficient then to bring in the Maryland claim without also having to then decide whether the violation of Maryland law itself would have constituted a crime or a serious crime?

MR. CARDOZO: Yes, Your Honor. But, of course,

the violation of Maryland common law is a personal injury tort of the type that is permitted to continue under FSIA. But even if it wasn't --

THE COURT: I'm jumping back there to the discretionary function exception. And if the test there is a serious crime has been committed, and if the serious crime is the allegation that there was a violation of the Wiretap Act, is that sufficient to pull in a Maryland common law claim?

MR. CARDOZO: Yes, Your Honor. And we see that in *Letelier*. In *Letelier* there was the wrongful death claim, the assassination itself, and then there was assault and battery. Assault and battery may not have been sufficient to pass the discretionary function, but the court allowed it to continue because of the more serious tort that occurred as well.

THE COURT: Can you respond to the defendant's argument about his inference that the original recipient of the e-mail was located in London and that there's not any allegation that the Ethiopian government was in any way involved in transferring that e-mail in London to the United States?

MR. CARDOZO: First of all, that's not what the e-mail says. It does not identify Mr. Kidane's acquaintances as being in London. And I'm not aware that that person was in London, frankly.

THE COURT: Do we know if the person was in the United States?

MR. CARDOZO: We do not. That's not alleged in the complaint, Your Honor, his location. And it's irrelevant because that's not the tort. The tort wasn't the sending of the e-mail, the tort wasn't even the opening of the e-mail, the tort wasn't even when Mr. Kidane opened the e-mail. The tort occurred after. The tort occurred after Mr. Kidane opened the Word attachment, his computer was infected, then Ethiopia forwarded the actual spyware to Mr. Kidane's computer, activated the infection, and began to wiretap his Skype calls. Each call that was intercepted was an individual tort. And the Wiretap Act recognizes this.

THE COURT: Was each call separately authorized under your view of the facts? And was there some affirmative action that was taken? Or once the malware was installed, was it just automatic at that point?

MR. CARDOZO: For each call, no, they were not individually authorized, it was automatic. However, because of the way that the licensing -- that the pricing schedule for FinFisher works, Ethiopia began to pay for that seat, that target seat of the spyware only when the -- Mr. Kidane's infection became active, and paid for it continuously until March of 2013 when they were caught red handed by Citizen Lab. Five days after that Citizen Lab

report Ethiopia pulled the plug on Mr. Kidane's infection and stopped paying. And that's when the tortious activity stopped.

THE COURT: Under your view of the facts, did the Ethiopian government need to engage in some affirmative act to turn on the spyware on the plaintiff's machine?

MR. CARDOZO: Yes, Your Honor. And that's what we allege in the complaint and that's what the brochures that we have attached from FinFisher support.

THE COURT: Would they have known and do the allegations support whether they would have known that they were turning it on on the plaintiff's machine, versus the person's machine who may have forwarded the e-mail to the plaintiff?

MR. CARDOZO: They certainly knew it was in the United States. Mr. Kidane's IP address would have made that abundantly clear. Whether they knew who it was immediately, that's something only Ethiopia can answer. However, the infection stayed live for four and a half months. They must have -- and we allege this in the complaint, they must have figured it out and they didn't turn it off until they were caught.

THE COURT: This question goes both to the entire tort, but also, I think, goes back somewhat to the discretionary function. The legislative history on the

discretionary function exception is quite limited and refers to a concern about traffic accidents in the United States. How do you reconcile that with the theory that does involve actions that, you know, span the globe at some level, as well as with -- let me ask you that first, then I'll ask you the follow-up.

MR. CARDOZO: That's *O'Bryan versus Holy See*, Your Honor. A policy that's formulated in the Vatican can be actionable under the Discretionary Act exception if it's applied in the United States. Globe-spanning suits are par for the course in Foreign Sovereign Immunities Act.

THE COURT: The second part of my question goes back to the concern I was expressing before about the discretionary function exception and potential for policy implications of a very narrow reading of the discretionary function exception. It is the fact that Congress was principally concerned with car accidents, some indication that Congress wasn't contemplating that they were authorizing actions against foreign states that could give rise to the type of potential foreign affairs concerns that I was raising before?

MR. CARDOZO: No, Your Honor, I don't believe so. And the courts have not -- you know, the court in *Letelier*, the court in *O'Bryan* recognized that there were potential diplomatic consequences.

THE COURT: Was that from *Letelier*? There had already been a prosecution in *Letelier*.

MR. CARDOZO: Indeed, Your Honor. But *Letelier* wasn't just between Cuba -- Chile and the U.S., but Cuba was involved as well. So this -- in *Letelier* it was even more of a globe-spanning situation than we have here.

THE COURT: What was the other case that you raised?

MR. CARDOZO: *O'Bryan versus Holy See*, it's -- *O'Bryan versus Holy See* is potentially the closest analogy we have in terms of the intent being formulated abroad and the application of that intent being actionable here.

Thank you.

THE COURT: I don't know if you had anything else. I was just looking down at my notes.

MR. CARDOZO: On location of the tort, Your Honor? No, only to reiterate that the tort -- both the Wiretap Act and the intrusion upon seclusion were -- began and ended here. And the fact that they were directed from abroad is irrelevant.

THE COURT: Is that true with respect to all of the intrusions you're alleging? I understand the point with respect to the Skype calls where, I take it, your argument is that someone remotely turned on the plaintiff's machine to store, to create, to make copies of those calls in a

portion of the computer files that were hidden from his views.

MR. CARDOZO: Yes. And the same thing happened with the web searches and e-mails.

THE COURT: That was my question.

MR. CARDOZO: Yeah. During -- while Mr. Kidane and, indeed, his family, including his children, were using the computer, the FinFisher software automatically activated, created copies of what they were doing, just like it did for the Skype calls, stored them on his computer and then, in the ordinary course of operation, would have sent them back to Ethiopia.

And to be -- so, in our papers -- defendant confuses this a little bit, so I want to make it quite clear. We're alleging a wiretap violation for the Skype calls and an intrusion upon seclusion action for the web searches and e-mails. So it's separate interceptions give rise to separate causes of action. The Skype calls might also gives rise to an intrusion upon seclusion case -- or, clause. But what we've claimed is that the Skype calls give rise to the Wiretap Act. And all of the conduct, including the Skype calls and the web search and e-mails give rise to intrusion upon seclusion.

THE COURT: Is there some reason you've pled this under the Wiretap Act instead of the Stored Communications

Act or the Computer Fraud and Abuse Act?

MR. CARDOZO: Your Honor, the plaintiff has chosen his causes of action quite carefully, and the reasons why we chose what we did is not something that I'm prepared to get into.

THE COURT: I'm not asking to get into your strategy. I was really more wondering whether there was something that went to the issues that we're talking about here. But I'm not asking for your strategy.

MR. CARDOZO: It's not having to do with the issues that we're talking about today.

THE COURT: Okay. That's fine. Okay.

Mr. Charrow, I think we've touched briefly on some of the other issues. But I want to make sure I've given you a chance to address everything you want to address. The issues that I still have left on my list that I will now put into a combined --

MR. CHARROW: I will try my best. A couple of points of clarification, if you don't mind.

THE COURT: Actually, just before you do that, I want the plaintiff to hear this as well, just the remaining issues that I have, which are damages for injury to a person, whether Title III applies to a foreign sovereign, question of whether there's an allegation of an intercept. As I said, I think we've touched on a number of these

points. Preemption. And the elements of the Maryland tort law in particular, whether the tort has to be directed at the plaintiff or whether there's some form of transferred intent.

MR. CHARROW: Let me start with that one, because I remembered, in May the --

THE COURT: I'm sorry. I forgot our break. We were to take a break. And I apologize, I was so engaged.

MR. CHARROW: No problem. How long?

THE COURT: Ten minutes.

(Pause.)

THE COURT: Mr. Charrow.

MR. CHARROW: Thank you, Your Honor. I would like to come back to one point that the court raised concerning place of injury.

THE COURT: Yes.

MR. CHARROW: If the court doesn't mind.

THE COURT: Not at all.

MR. CHARROW: And I would like to start with two things. First of all, I would like to look at the *O'Bryan* case which the plaintiff discussed. The *O'Bryan* case consisted of two genre of torts. There was the tort committed by the Holy See directly, in negligently training and negligently supervising priests that were sent from the Vatican to the United States. Very much like -- very much

like the virus being sent by someone from country A into the United States. The court held that the acts in Rome did not take place in the United States. Now, what about -- and, therefore, there was no waiver of sovereign immunity under 1605(a)(5).

What about the contention that the case against the Holy See was permitted to proceed with respect to other grounds? And that is true. But it was *respondient superior*, it had nothing to do with what the Holy See did or not do. It was purely vicarious liability. That was the basis of those claims that were permitted to go forward, and those with respect to the bishops in the United States who, indeed, were in a hierarchical religion, employees, if you will, of the Vatican.

The other case I would like to come back to just to discuss with the court is the *Four Corners* case. Let's change the facts somewhat to make it simpler. Let's make believe that the plane flew from Paris to Colorado, or a scheduled flight from Paris to Los Angeles, and let's make believe that the engines fail in Colorado. Okay? It's not a tort that necessarily involves state of mind, it's a defective engine. The defect occurred in France. No waiver of -- or, no waiver of immunity under 1605(a)(5) because the entire tort did not occur in the United States, even though the infliction of the injury did occur in the United States.

And I think that phrase was precisely the phrase used by the *Jerez* court.

What if, rather than having a defectively designed engine, we have a worker who is dissatisfied with his lot in life and decides to attach a bomb to the engine. And he did that while the engine is being -- while maintenance is being conducted on the engine. And now the plane takes off, bound for the United States, bound for Los Angeles, explodes over Colorado. Different result? I think not.

I don't think the intent would make any difference one way or the other. The acts of setting the plane in motion occurred overseas, that's where the tort occurred, that's where the *Four Corners* held the tort occurred. And indeed, arguably, that's dicta of what the *Perez* court held. The infliction of the injury occurred here, but that's not enough.

THE COURT: I take it then you would reject the examples given in the dicta that we're talking about from the D.C. Circuit from a year or so ago?

MR. CHARROW: No, I'm reading from that. That's exactly what I'm reading from. I think that dicta is consistent with what I'm talking about.

THE COURT: It was *Jerez*, and they -- the court there, I thought, suggested that there would be a claim for someone mailing anthrax or a bomb to the United States.

MR. CHARROW: The infliction of the injury would occur in the United States. They didn't say one way or another, they just said it was different than -- or, different from, to be grammatically correct.

THE COURT: Which is the reason I think it's dicta. But I think the implication of what they're saying --

MR. CHARROW: I think it's less than dicta. I think the court wasn't grappling one way or another, but was contrasting it to what did or didn't occur in the case.

If you look at the Colorado case, if you look at the *O'Bryan*, all of these cases point to the very simple proposition that if you start something in the foreign country and it ends up in the United States, but the acts itself started in a foreign country, that is not enough to trigger the exemption under 1605. Which makes sense, given the original nature of 1605(a), what it was designed to accomplish and what it was designed not to accomplish.

THE COURT: You mean car accidents?

MR. CHARROW: Yeah, rudimentary torts. There are a couple of other points that I think are worth mentioning, and I'll forget if I don't address them in this order. So if the court has an objection, please let me know.

There was some -- the court questioned the plaintiff concerning whether they would have -- whether the

defendant would have known that it, in fact, was in the plaintiff's computer. And the response was they must have figured it out. That's a quote from the plaintiff during oral argument. And they pay for licenses and, therefore, as they pay more, they must have known.

In fact, according to the complaint, at paragraph 45, they paid for a fixed number of licenses. So as long as you aren't above your threshold, the payment rate -- the amount you pay does not increase.

THE COURT: I thought what Mr. Cardozo indicated to me was that as alleged, the Ethiopia government would have actually had to affirmatively turn on their surveillance and that they would have known that it was in the United States because they would have recognized it as a US IP address, even if they weren't sure, didn't know that the -- it was the particular plaintiff whose machine they were turning on.

MR. CHARROW: I'm sorry. I didn't see that in the complaint.

THE COURT: Well, I'll have to take a look and see if that's there.

MR. CHARROW: I did not see either allegation in the complaint. I may have missed it, but I don't remember seeing either of those allegations in the complaint. What I do remember, however, are the actions of the plaintiff

prior, long before this hearing, that would be inconsistent with knowledge on the part of Ethiopia.

For example, the plaintiff is proceeding under a pseudo name. Now, if Ethiopia knew that it was monitoring the plaintiff's computer, they would know who the plaintiff was. But the plaintiff is proceeding under a pseudonym, so clearly the plaintiff assumes that the government doesn't know who he is. That would be inconsistent with the statements made during the oral argument today. And there are no statements that I've been able to find in the complaint that would be inconsistent with the petition filed to proceed under a pseudo name.

THE COURT: Okay.

MR. CHARROW: Okay. Now, you have a list of order you would like me to go through. You want to talk about transferred intent?

THE COURT: Sure.

MR. CHARROW: Transferred intent is real simple. Restatement Second discusses, in the comments to the intent sections, which would be the single digit sections, and Restatement Third, tentative draft one was just voted on by ALI in May, and under section 110 it discusses transferred intent. Makes no change to transferred intent under Restatement Two. But let me talk about Restatement Three because I'm more comfortable with it. It would be section

110. It would be section 110 of the tentative draft. That was, in fact, passed by ALI in May.

Transferred intent only applies to assault, to a battery, to false imprisonment. It does not apply beyond those three torts. It does not apply to invasion of privacy. End of story. So, if the plaintiff is relying on transferred intent, it's inapplicable.

THE COURT: What about plaintiff's analogy that if you have somebody who's peeking in somebody's window and they think they're peeking in somebody else's window, doesn't really matter, they're still engaged in an invasion of privacy.

MR. CHARROW: But that's not the way the tort reads. 652B does not read that way. And 652B is what is being relied upon by the plaintiff in this case. And 652B deals with an intent to intrude upon the seclusion of a person and injury to that person. It is the same person. Transferred intent has no place in intrusion upon seclusion, at least under the Restatement view. And, of course, the plaintiff is relying on the Restatement for the underlying tort. So all the baggage of the Restatement necessarily comes along with it, including the limitation on transferred intent under 110.

THE COURT: Okay.

MR. CHARROW: The Wiretap Act, I mentioned to the

court that in my view there was no violation of the Wiretap Act as pled. And I base this on two reasons. First of all, as the Court alluded to earlier in the day, section 2520, which provides the private right of action in this case, deals with persons and entities. But 2520 gives the private right of action for a violation of the provisions of the Wiretap Act. And the provision of the Wiretap Act relied upon by the plaintiff in this case is 2511. 2511 deals with person, not persons or entity. And persons are traditionally viewed as nongovernmental entities.

Now, here the Wiretap Act defines a person to include federal government and local and state governments, but it does not define -- does not define it to include a foreign nation. And foreign nations are referred to throughout the Wiretap Act under other provisions. So the fact that foreign nations were mentioned by Congress is strong evidence that person is intended to exclude foreign nations, at least in 2511.

THE COURT: So what is that -- what work does the word entity do in 25 --

MR. CHARROW: There are other provisions of the Wiretap Act that do deal with entities. And 2511(a) and similar sections do not; they are limited to persons. So the Wiretap Act does not apply to foreign governments.

THE COURT: So what are the provisions that deal

with entities? Like the provision that deals with manufacturing devices?

MR. CHARROW: Let me see if I can find it. There is a provision (3)(b) which would be -- yeah, I'm sorry, 2511(3)(b), a person or entity providing electronic communication services. (3)(a), except as provided in paragraph (b) of this section, a person or entity providing electronic communication service.

So the word entity is used -- and these provisions, obviously, aren't applicable here, but these provisions are used -- person or entity is used in 2511. It is not used in the provision of 2511 on which this complaint is based, though.

THE COURT: Are the provisions that you just read to me actually ones that give rise to liability? I think it's (3)(a), looks like it is.

MR. CHARROW: Um-hum. Yes.

THE COURT: Okay. So, the definition of person actually doesn't include the United States, it includes an agent, an employee or agent of the United States. And section 2712 creates a cause of action against the United States for violation of section 119 -- or, Chapter 119, which is the Wiretap Act.

So, under your theory, if entity -- under your theory, if a violation of section 2511 is limited to a

person, and the United States is not a person in the same way that a foreign government is not a person --

MR. CHARROW: I don't follow that, Your Honor. 2511 deals with local and state governments, it deals with agents of the United States, does it not?

THE COURT: Right. But is there anywhere in 2511 where it actually suggests that the United States itself would be subject to suit?

MR. CHARROW: No. I misspoke then.

THE COURT: It doesn't impose -- I mean, the same way 2511 doesn't, on it's face, impose any duty on a foreign sovereign, it doesn't impose any duty on the United States.

MR. CHARROW: The basic rule, obviously, if you go back to the Dictionary Act, and even this law is that a person does not include sovereigns. Here there's a peel-back of that for states and local governments, and later on for the U.S. government.

THE COURT: But it's not a peel-back for states.

MR. CHARROW: It is a peel-back for states.

THE COURT: I'm sorry. It's not a peel-back for states or the federal government. It's a peel-back for an agent -- in fact, it's a peel-back not for the state, it's for their -- a person is an employee or agent of the United States or any state. So it's not a peel-back for, literally, for the states themselves.

MR. CHARROW: But their employees.

THE COURT: But their employees.

MR. CHARROW: Correct.

THE COURT: So, is it your position then that an employee of a foreign government isn't subject to the Wiretap Act, the individual, him or herself, if they're acting, you know, as an employee of their foreign government?

MR. CHARROW: They probably would not be subject to the Wiretap Act, but that's not before the court.

THE COURT: I think maybe it is before the court because the question is whether, as I take it from what the parties were discussing, is whether a serious crime has been committed and if there was some agent -- obviously, no government acts without agents. And so the question is whether there's some person who committed a crime in some way, right?

MR. CHARROW: You would be reading out of the fundamental definition of person, the concept that it does not apply to governments presumptively, by having it apply to their employees. Indeed, if you sue someone under the Federal Tort Claims Act as an employee, what happens? The federal government intervenes.

THE COURT: That's true. But that's under --

MR. CHARROW: You cannot sue, quote, an employee

of the United States as an employee.

THE COURT: You can, but the United States is then substituted in under the statute.

MR. CHARROW: Correct. That's correct.

THE COURT: If the United States concludes that they were acting within the scope of their duties. Okay. Well, I understand your argument. Thank you.

MR. CHARROW: Okay. We don't believe there was an interception either, because an interception, in our view, requires contemporaneous interception. And I think there are a number of courts that have so held. And there's a split among the circuits. And the D.C. Circuit has not opined on this, to my knowledge.

THE COURT: But even taking the view that an interception is contemporaneous, I thought that the plaintiff's allegation is that in fact what was occurring here is the computer is being highjacked and is creating an instantaneous or simultaneous copy in an area of the files which is not generally perceptible to the user of the computer.

MR. CHARROW: That's exactly what happened in the *Bunnell* case.

THE COURT: In which case? *Bunnell*?

MR. CHARROW: Precisely what happened in *Bunnell*. And there the court held that there are two laws, there is

Title I and Title II. Title I is the Wiretap Act, and that's the one before the Court. And Title II is the Storage Act, and that is not before the court. And the court said the two are mutually exclusive. And it held there that the fact that something is -- there I believe the hacker programmed the computer to make a copy of all of the computer's e-mail and then sent those e-mails on to the hacker.

THE COURT: That's a different circumstance because the e-mails already reside on the computer and e-mails typically are treated as stored communications and, therefore, subject to the Stored Communications Act. Whereas, a Skyped call is not stored on the computer in the same way that an e-mail is stored and that it -- the allegation is that the call -- that a copy of the call was made in real time on the computer. With respect to an e-mail, the e-mail is residing on a server somewhere, it's residing on the computer somewhere. You're making a copy of the stored communication. But with a Skype call, I take it the allegation is that as the call is occurring, it's being recorded.

MR. CHARROW: But there really is no difference technologically between a Skype call when seen by a computer and an e-mail when seen by a computer. They're both subject to protocols for reassemblage and they're identical.

THE COURT: I would have to get back and look at the -- technologically, the case that you looked at. But technologically I don't think that they are identical because I think that the e-mail resides on your computer. And maybe -- there might be a period of time, I guess, if you intercepted the e-mail precisely as it was arriving, which it might be treated as an interception.

But if I've got 100 e-mails on my computer and someone comes in and copies those e-mails off my computer, they're copying a stored communication because they're on my computer. That's different than if I'm using my computer for a Skype call, where it's in real time, there's nothing that's stored on my computer, but they are making a copy of it where it's not stored on the computer, that actually would be occurring in real time in a way that an e-mail already resides there and is already sitting on the computer and is then copied.

MR. CHARROW: From a technological point of view I see no distinction between Skype and e-mail, number one. But more critically from a legal perspective, I don't see a distinction between whether a person goes in through hacking and forces another copy to be made and then redirected versus coping something that may not otherwise be copied onto the computer and then redirecting it. There is no difference between the two. There are no devices being

planted in the machine, there's just a virus, which is software.

THE COURT: I'm not aware of any case that has ever held that you could do this before. But I understand their theory, which is that allegedly the defendant was using the plaintiff's computer as a recording device and was intercepting the communication as it was occurring and recording it on the plaintiff's own device, unbeknownst to the plaintiff.

MR. CHARROW: From a technological point of view, as far as -- you know, as far as I understand e-mail and Skype, they're subject to protocols that break down the message, whether it's an e-mail message or Skype message, into packets and are reassembled at the other end.

THE COURT: That's when they're being transmitted.

MR. CHARROW: Correct.

THE COURT: But here the e-mails, as I might have -- based on your description of the case you're describing, is e-mails are actually sitting on the computer. And that's why it's a stored communication, it's actually sitting there on your computer and someone has to go in and copy it off of the computer where it's already stored, versus a Skype call is not stored on the computer unless someone actually creates a copy of it. If they're creating a copy, which they're saying constitutes a violation --

MR. CHARROW: Their allegation is transforming Skype into an e-mail is an element that creates a violation of the Act.

THE COURT: Making a real time copy of Skype is what constitutes --

MR. CHARROW: Onto the very computer owned by the plaintiff.

THE COURT: That's my understanding, that's their allegation. As I said, I'm not aware of a case that says that, but I conceptually understand the point.

MR. CHARROW: Nor am I.

THE COURT: Did you have more?

MR. CHARROW: Third aspect --

THE COURT: Yes.

MR. CHARROW: -- of the Wiretap Act are two forms of preemption. I'm only going to discuss one here because the other is discussed thoroughly in the brief we discuss. Express preemption. But merely because something expressly preempts does not preclude it from also impliedly preempting, as the court held in *Buckley*. And telecommunications, especially these laws, we view as field preempting. They would preclude the states from entering into similar laws because they, in fact, field preempting, states do not have the traditional type of law making responsibility in this area as the federal government has.

THE COURT: Doesn't virtually every state have its own Wiretap Act?

MR. CHARROW: Every state has its own Wiretap Act -- most states do, I wouldn't say every one.

THE COURT: I don't know. I don't mean to suggest every one, but many states do.

MR. CHARROW: Many states do and most of those states are -- most of those laws are criminal.

THE COURT: Okay.

MR. CHARROW: And when we're talking about civil remedies, that's when we're talking about preemption.

THE COURT: Why would that be different?

MR. CHARROW: Because there's nothing that precludes the federal government -- because normally when you're talking about preemption, you're talking about civil actions that affect conduct in the civil arena. Which sounds circular, I know, but I've never seen preemption in the criminal arena, per se; doesn't mean it doesn't exist. But, as a general rule, we're talking about in the civil arena, and here we're talking about in the civil arena.

And the general rule is that, okay, we're looking at telecommunications. Telecommunications have been within the purview of the federal government since the original act was passed in what? 1934? Communications Act.

THE COURT: Yes.

MR. CHARROW: Okay. States have only been able to deal with communications, telecommunications on an intrastate basis. They have only been able to deal with it beyond an intrastate basis when they're permitted to do so by the federal government. So unlike normal cases of preemption, here the default is not state law governs unless the federal government says to the contrary, the verse is true; federal law pertains to interstate and foreign communications unless -- federal law governs unless the federal government gives the state the ability to something.

THE COURT: The plaintiff cites three or four District Court decisions in their brief saying there's no preemption, and I don't recall your citing any authority.

MR. CHARROW: We did. The *Bunnell* case discusses it.

THE COURT: It says that there is field preemption.

MR. CHARROW: Both field preemption and express preemption. Both.

THE COURT: Okay. You know, I mean, for example, there are a number of states that have two-party consent requirements. Whereas, the Wiretap is a one-party consent requirement. Is it your view that all those laws are preempted and that you only need one party consent to intercept a telephone call in all those jurisdictions, to tape a call?

MR. CHARROW: I guess the question remains, does

the state have the permission of the FCC to do it? And my bet is they do.

THE COURT: Okay.

MR. CHARROW: It's very much like the Food, Drug, and Cosmetic Act, there's a broad preemption provision in section 521 of the FTCA --

THE COURT: Implied preemption requires that the state laws frustrate the purpose, at a minimum, of the federal law. How would any of these state laws frustrate the purpose of the federal law here by being more restrictive?

MR. CHARROW: Let's go back a moment. That's only one aspect of it. There's different types of implied preemption. In field preemption the government occupies the entire field.

THE COURT: Field preemption, there are maybe four areas that the Supreme Court has ever recognized for field preemption. This is not one of them.

MR. CHARROW: I beg to differ with you. It is, in fact, because we're dealing with foreign commerce.

THE COURT: So you're making a different argument. So you're arguing more commerce preemption.

MR. CHARROW: Well, you asked me about preemption, and I was relying on Article 1, Section 8, Clause 3. The only reason that states have authority to act in this area

is if it's given to them by the federal government.

THE COURT: I thought you were relying on the supremacy clause.

MR. CHARROW: I am relying on the supremacy clause, but it's the supremacy clause vis-à-vis the commerce clause.

THE COURT: But it's not based on the Wiretap Act, it's based on Congress's exclusive power to regulate foreign commerce?

MR. CHARROW: Correct. That's the field preemption.

THE COURT: That's not in the briefs.

MR. CARROW: I know that.

THE COURT: Okay.

MR. CHARROW: I'm aware of that.

THE COURT: Okay.

MR. CHARROW: Anything else?

THE COURT: Let me see.

No. I think that covers the questions I had.

MR. CHARROW: Okay.

THE COURT: Thank you.

MR. CARDOZO: Your Honor, to return for a moment back to comity. The FSIA was designed to remove foreign sovereign decisions from the executive branch. And just a couple of years ago, in 2012, the Supreme Court, in *Samantar v. Yousuf*, told us that pre-FSIA common law tradition was

based on the executive suggesting in individual cases whether to apply comity and to dismiss the case as a Foreign Sovereign Act, or to allow the case to go forward.

The FSIA, according to the Supreme Court in 2012, was designed to supplant the executive acts -- or, the executive branch's judgment in that case and give the judgment to this Court, to courts in the FSIA.

THE COURT: That's true, but a little bit circular in that the Court has to then figure out what the scope of that authority is that Congress has given to the Court. And the question is would Congress have intended to give the Court the authority to do something that would have, potentially, significant foreign policy consequences, where the legislative history suggests that Congress was principally concerned -- or, at least first concerned with auto accidents.

MR. CARDOZO: True, Your Honor. However, the courts certainly have not limited FSIA to auto accidents. Second -- actually, two other points. Plaintiff is unaware of any case where any federal court has dismissed for comity. Hasn't happened, to our knowledge. And second, if it did become a problem and we saw plaintiffs subpoenaing foreign ministers, then either Congress or the executive could step in. And if our discovery requests went out of order, the State Department might well do so in this case.

THE COURT: What way would they be able to step in?

MR. CARDOZO: To file a statement of interest or to intervene to protect the U.S.'s foreign diplomacy powers.

THE COURT: But what --

MR. CARDOZO: We haven't seen it. It's never happened.

THE COURT: So we don't know what theory they would assert. They would intervene or file a statement of interest, but we don't know what they would be able to point to as their basis for telling the court please don't do that.

MR. CARDOZO: Comity would be the --

THE COURT: That's what I was wondering, whether there's some Constitutional comity principle that might govern these cases at some level.

MR. CARDOZO: In a sense, that's a Constitutional principle. But comity is a pre-Constitutional common law principle.

THE COURT: Okay.

MR. CARDOZO: So to turn to the Wiretap Act issue, which my opposing counsel talked about at length.

From the statute, any person whose communication is intercepted may recover from any entity that engaged in the interception. Here, there was an interception. I think Your Honor quite succinctly described our theory of the case here, about how the software residing on Mr. Kidane's

computer, copied in real time, which is something very different than what happened in the *SCA* case. So there was an interception.

THE COURT: Is that all in the complaint, by the way? I think your colleague indicated -- he wasn't sure whether it was.

MR. CARDOZO: Yes, Your Honor, it is in the complaint. And I think it shows most strongly in the summary of allegations, toward the end, and then in the first cause of action --

THE COURT: Okay.

MR. CARDOZO: -- we describe what happened.

THE COURT: Okay.

MR. CARDOZO: And we talk about it, as well, in the opposition to the motion to dismiss.

But, the Second Circuit, in *Organización JD Ltda. versus DOJ*, told us that entities, as in 2520, must mean governmental entities. And as Your Honor pointed out, entities are not liable under 2511(a). The only entity that is directly liable under 2511 is a service provider. If Congress had meant to limit entity in 2520 to service providers, they would have done so. Instead, they excepted the U.S. government from 2520.

So 2520 has both *Organización* and *Adams versus City of Battle Creek* in the Sixth Circuit, held the 1986

amendment adding the word entity must mean that governmental entities are liable under the act.

THE COURT: I suppose, given the definition of person, even a service provider?

MR. CARDOZO: A service provider is definitely a person, Your Honor.

THE COURT: So what, then, does the word -- adding entity add, if a service provider is already a person?

MR. CARDOZO: So there are also governmental service providers, I think that's the issue. There are service providers that are persons and there are service providers that are nonpersons service -- you know, the internet is a weird place and there are service providers that fill both those roles.

But 2520 creates the cause of action to recompense plaintiffs who have suffered an interception. And that's what happened here. And it's almost that simple. And adding the word "or entity," as courts in civil circuits have held, meant that Congress intended governmental entities to be liable.

THE COURT: What about the preceding question though, of whether an agent of a foreign government would actually be subject to criminal liability under 2511?

MR. CARDOZO: I see absolutely no reason why that wouldn't be true.

THE COURT: But 2511 only applies to a person, and a person is defined as an employee or agent of the United States or any state or political subdivision thereof, doesn't say --

MR. CARDOZO: Or a natural person, an individual. When individuals are prosecuted by the United States they're not prosecuted as -- under a theory of *respondient superior*, they're prosecuted as themselves, as individuals. And there's no reason to think that whichever agent of the Ethiopia government actually supervised the surveillance on Mr. Kidane would not be subject to prosecution.

Congress knew how to exempt the U.S. government from 2520 and they could have exempted foreign sovereigns as well. They didn't. They chose not to. In *Bunnell*, the case that opposing counsel cites, I think opposing counsel may misapprehend the technology at issue in *Bunnell*. The access was to files, was to already stored communications. And that's not what happened here.

I think Your Honor -- I think Your Honor apprehends plaintiff's argument in this case.

Shall I turn to preemption, or do you have any --

THE COURT: That would be fine.

MR. CARDOZO: Okay. In preemption -- *Leong versus Carrier IQ* out of the Central District of California shows that 2518 doesn't impact preemption. It only discusses what

federal remedies are available. And the two sets of facts that we're talking about are distinct. So our Wiretap Act claim is limited to the Skype calls. Our intrusion upon seclusion claim encompasses the Skype calls, but focuses on the web search and e-mail monitoring. We have a little bit less technical information about how exactly that happened, but we do know it happened and we've alleged it quite clearly in the complaint.

So even if there is preemption, which there isn't, and *Leong* teaches us that there isn't, the preemption would only be regarding the Skype calls and it would not preempt the entirety of our claim because we're talking about different courses of action and different modules, actually, of FinFisher that did the recording.

THE COURT: But if -- never mind. I follow.

MR. CARDOZO: Your Honor indicated --

THE COURT: I guess, let me break this down. This goes back to the question I think I was asking earlier, which is whether a criminal violation -- or, an alleged criminal violation of the Wiretap Act is enough to get your foot in the door to then assert, notwithstanding Foreign Sovereign Immunities, your intrusion upon seclusion claims, if you're breaking those claims down in a way in which they actually are focused on something different than what you're focusing on in the Wiretap Act claims, does that mean that

the Court has to find some other basis of not applying the discretionary function exception as to that portion of the claim because it's not -- there's no allegation of criminality there?

MR. CARDOZO: No, Your Honor. The FSIA gives this court jurisdiction not over individual claims, but if you look at the language, it gives this court jurisdiction over the case, and the case is composed of all of its claims. And defendant has cited no authority, at least not that I was able to grasp, that would require this Court to dismiss the intrusion upon seclusion claim --

THE COURT: Okay.

MR. CARDOZO: -- if the entire case goes forward.

Your Honor, before the break, indicated that the Court had questions regarding damages for injury to a person. And I don't think opposing counsel mentioned that. Does Your Honor --

THE COURT: I was really cataloging the arguments that I think the parties had raised in the case and making sure everyone had an opportunity to address those. I don't have particular questions about that one.

MR. CARDOZO: I would just reiterate, under both D.C. and Maryland case law, privacy torts are per se injuries to a person, and that's what we have alleged here.

Thank you.

THE COURT: Did you have anything further on the preemption argument, on the field preemption argument?

MR. CARDOZO: No, Your Honor. I think that this is not a case where field preemption exists. And *Leong versus Carrier IQ* in the Central District of California supports us.

THE COURT: Okay. Thank you. Anything further? Are you tired?

MR. CHARROW: Two hours and 20 minutes.

THE COURT: I thank you all. This has been extremely helpful for the Court. And I apologize for keeping you so long. But, actually, both arguments were very, very helpful and have helped me at least beginning to formulate my views on this. And I'll do my best to provide a decision as soon as I can. I still want to mull over the question of whether I should at least give the United States an opportunity to be heard, if they want to be heard at this stage.

I recognize that they often wait to be heard in the Court of Appeals, which puts District Courts in the awkward position of not having all the arguments in front of them that may actually be before the Court of Appeals when the Court of Appeals decides a case.

So I'll mull that over and render a decision on that, render a decision on the merits as soon as I can.

MR. CHARROW: Your Honor, we had a recent experience with the Department of Justice and they said wait until the case gets to the Court of Appeals.

THE COURT: Okay. All right. Anything further?

MR. CARDOZO: Thank you.

THE COURT: Thank you. Thank you all.

* * *

CERTIFICATE OF OFFICIAL COURT REPORTER

I, JANICE DICKMAN, do hereby certify that the above and foregoing constitutes a true and accurate transcript of my stenograph notes and is a full, true and complete transcript of the proceedings to the best of my ability.

Dated this 27th day of July, 2015.

/s/_____

Janice E. Dickman, CRR, RMR
Official Court Reporter
Room 6523
333 Constitution Avenue NW
Washington, D.C. 20001

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JOHN DOE, a.k.a. KIDANE, Plaintiff, v. FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA, Defendant.	Civil Action No. 14-372 (RDM)

NOTICE BY THE UNITED STATES

On July 15, 2015, the Court notified the United States that the above-captioned case "may present 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)," and asked whether the United States "wish[es] to be heard on these issues at this stage of the litigation." *See* Notice, ECF No. 35. The United States hereby advises the Court that it respectfully declines to file a Statement of Interest in this matter at this time. *See* 28 U.S.C. § 517.

The United States appreciates the Court's invitation and the additional time that the Court afforded the United States to consider the matter.

Respectfully submitted this 25th day of September, 2015,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

RONALD C. MACHEN, JR.
United States Attorney

ANTHONY J. COPPOLINO
Deputy Director

s/ Michelle R. Bennett
MICHELLE R. BENNETT (CO Bar No. 37050)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue N.W. Room 7310
Washington, D.C. 20530
Tel: (202) 305-8902
Fax: (202) 616-8470
Email: michelle.bennett@usdoj.gov

Attorneys for the United States of America

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JOHN DOE, a.k.a. KIDANE,
Plaintiff

vs. Civil Action No. 14-372 (RDM)

FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA,
Defendant

NOTICE OF APPEAL

Notice is hereby given this 22nd day of June, 20 16, that

JOHN DOE, a.k.a., KIDANE,

hereby appeals to the United States Court of Appeals for the District of Columbia Circuit from the judgment of this Court entered on the 25th day of May, 20 16 in favor of FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA against said JOHN DOE, a.k.a., KIDANE.

/s/ Nathan Cardozo
Attorney or Pro Se Litigant

(Pursuant to Rule 4(a) of the Federal Rules of Appellate Procedure a notice of appeal in a civil action must be filed within 30 days after the date of entry of judgment or 60 days if the United States or officer or agency is a party)

CLERK Please mail copies of the above Notice of Appeal to the following at the addresses indicated:

Robert P. Charrow
Thomas R. Snider
GREENBERG TRAURIG, LLP
2101 L Street, N.W., Suite 1000
Washington, D.C. 20037
Counsel for Defendant Federal
Democratic Republic of Ethiopia