UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against- **Case No. 12 Cr. 185 (LAP)**

JEREMY HAMMOND,

Defendant.

EXHIBIT I
EMAIL FROM "hyrriiya"

From: [redacted]
Subject: **Re: Pertaining Jeremy Hammond case**
Date: May 7, 2012 12:09:00 PM EDT
To: Sarah Kunstler [redacted]

Thank you for the prompt reply.

This is the e-mail I wrote for whomever is the lawyer of Jeremy Hammond, in this case I think Elizabeth Fink is so please forward this to her as it pertains to exculpatory evidence on Jeremy's case.

I will listen to this email address I'm writing from for the next 7 days, so I am available to answer questions in this time period.

take care.

PS: dear FBI/NSA/SS agent reading this, good luck finding me. it's early morning in this timezone.....

Dear Ms. Elizabeth Fink:

I am a hacker that had extensive interaction with both Sabu and Hammond in relation to the Stratfor hack. At all relevant times to the Stratfor hack and my relations with those two men, my online "handle" was "hyrriiya." I believe that I have some important information that may shed exculpatory light on the federal allegations that your client was the one who found, perpetrated and fully exploited the hack on Stratfor.

Prior to my interactions with your client, I was involved in multiple Anonymous "operations" to assist freedom fighters and protesters engaged in the Arab Spring uprisings.

In mid-to-late 2011, I read an article from Stratfor concerning Anonymous and Mexican drug cartels. Upon reading it, it became clear to me that Stratfor must have people inside Anonymous who serve as informants to the firm. After this realization, I became deeply interested in compromising Stratfor's systems and communications in order to identify possible Anonymous informants and expose them to the rest of the movement.

By sheer accident, on or about November 7, 2011, I compromised two of Stratfor's database services due to them simply not having passwords to protect administrative access. This simple mistake on their part allowed me access to all

of Stratfor's systems and client information. (It would be worth looking into industry standards for security, as I firmly believe Stratfor failed to meet a few of them and thus bears some onus for the compromise of sensitive customer data.)

This initial hack of Stratfor occurred approximately TWO week BEFORE anyone involved in #antisec (including Sabu and Hammond) had ANY knowledge or involvement in Stratfor. After reviewing the data I was able to access in Stratfor, I realised that the customer details included all pertinent credit card information for both individuals and a multitude of corporate entities, military institutions and espionage agencies. Upon this realisation, I promptly decided that I wanted this information to be public, so as to deliver a big "f*** you" to them.

At the same time, I knew that I also wanted to befriend Sabu and the #Antisec participants so that I could infiltrate them and identify who they are. With this goal in mind, first I contacted Sabu and discussed the details of the hack in Private Message (PM) on irc.cryto.net. After I spoke with Sabu and he offered that it would be best if Stratfor was an #Antisec hack, I joined the private IRC #Antisec channel (called #antisec on irc.cryto.net) and started to drop bits of Stratfor customer data. As I hoped, I grabbed their attention immediately by dropping credit card information directly from the Stratfor database about military intelligence agencies, as well as other previous targets of #Antisec and Lulzsec. This occurred on or about NOVEMBER 15-21, 2011.

Sabu, who we now know was an FBI informant and whose computer was under constant federal surveillance, seemed extremely impressed by the information that I had obtained from Stratfor. Accordingly, I saw my goal of getting closer to him as becoming accomplished. As such, I gave Sabu and other #Antisec participants full information on how to access Stratfor servers and information by posting it on their main IRC channel (#antisec). To my observation and knowledge, it seemed that Sabu took a leadership role once the information was posted, making other special, private channels and directing certain individuals in #Antisec (including your client Hammond) to take my work and develop it further, including accessing and copying Stratfor's mail spools and leaking client data.

Unfortunately, due to good operation security procedures (we call it "opsec"), personally I do not maintain any records or logs from IRC, and as such, I cannot provide you with hard evidence to back up what I am disclosing to you. HOWEVER, as it has been repeatedly disclosed by the FBI itself that since Sabu's arrest, he had surveillance and monitoring equipment on his laptop recording ALL of his communications, it stands to reason that all of what I said above MUST be a part of the evidence that the FBI currently have.

As this evidence would be exculpatory to your client (demonstrating that he did not do the substantive hack of Stratfor as charged), I know that you should be

able to request it from the prosecuting AUSA during the Discovery phase of your client's trial. I would advise you to request all logs of the #antisec main channel on irc.cryto.net (Sabu was ALWAYS in it, so he logged most of the channel's entire communications). I would say the relevant time period to request said logs would be between November 07, 2011 - March 5, 2012 (or whenever Sabu stopped logging after being outed as an informant). I also spoke with Sabu at length in Private Message on irc.cryto.net, and as such, the FBI should have complete logs of my PMs with Sabu regarding the Stratfor hack as well.

Again, I firmly believe that this information will constitute exculpatory evidence and the AUSA has no right to withhold it from the defence. I believe that these facts can and will alleviate some blame from the defendant hence why I am contacting you.

Moreover, I would point you to a close and thorough examination of the timeline of the alleged Stratfor hack and the later information dumps from #Antisec. If Sabu knew of the hack when I disclosed it to him, and if Sabu knew (which he did as the logs will show) that #Antisec was going to dump multiple loads of sensitive customer data in its "LulzXmas" releases since he was the main organizer of this event, then as Sabu's machine was logged by the FBI, it can be STRONGLY implied that the FBI knew of all of this as well. The question then arises, to what degree of fault does the FBI have in allowed the CONTINUING hack of Stratfor, theft of customer information, copying of personal email spools, and dumping of such information to the public. From the very DAY that I disclosed the Stratfor hack to Sabu, the FBI would have had knowledge of it from their logging of Sabu's computer (they maintain in news stories that they had a very close working relationship with the informant and that he reported vulns and hacks received on a daily basis). This means the FBI allowed the entirety of the Stratfor hack to go forward, under its oversight.

In conclusion, I am stating and admitting, AS FACT, that I was the person who hacked Stratfor and who subsequently provided the details and access to Sabu through both private PMs with him and in the #Antisec main channel on irc.cryto.net. Your client only later worked on Stratfor per request and direction of Sabu and only after I had accessed all relevant sensitive client information and databases.

Please tell Mr. Hammond that he is a true friend and that I have great joy in having met him. He is a kind, friendly, caring person who is passionate for creating the change he knows that we need in this world. I have nothing but the utmost respect for him, and I am extremely saddened to see the prosecuting AUSA trying to slam him with harsh charges that carry strict sentences, in an effort to make an example of him to other Anons.

It is a great shame that he was betrayed by Sabu in such an under-handed manner, and I wish to do what I can to point you in the correct direction to try to remedy anything you can of this situation.

Best wishes,

hyrriiya