UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA Plaintiff, v. MARTIN GOTTESFELD, Defendant.	Case No.: 16-MJ-4117 (MBB)

MARTIN GOTTESFELD'S MOTION FOR RELEASE ON CONDITIONS

Martin Gottesfeld, through counsel, requests this Court release him on the proposed conditions below which will reasonably assure his appearance in court. *See* 18 U.S.C. § 3142(f). The charge Mr. Gottesfeld faces carries no rebuttable presumption of detention. *See* 18 U.S.C. § 3142(e). Mr. Gottesfeld poses no danger to the community, nor did the government argue that he poses one at the April 27, 2016 detention hearing in this matter. The only question is whether Mr. Gottesfeld is a serious flight risk such that there is no condition, or set of conditions, that could reasonably assure Mr. Gottesfeld's appearance in court. The release conditions proposed below, in conjunction with the application of the factors articulated in 18 U.S.C. §3142(g) and well established 1st Circuit case law, establish that release is appropriate.

FACTS

Mr. Gottesfeld was charged in a criminal complaint of violating federal conspiracy law under 18 U.S.C. § 371, with underlying allegations he conspired to violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"). The Court detained Mr. Gottesfeld on or about

February 17, 2016. On April 27, 2016 the Court held a detention hearing at which both sides presented arguments and submitted evidence. At the close of the hearing, Magistrate Judge Bowler took the matter under consideration. It is now over two months later and no decision has been forthcoming. This motion follows.

NATURE OF ALLEGED OFFENSE

Mr. Gottesfeld is charged with a single count of conspiracy for allegedly conspiring to cause unauthorized damage to protected computers. *See* 18 U.S.C. § 1030(a)(5)(A); Aff. of Michael Tunick (ECF 3-2) ("Tunick Affidavit") at p. 1 (Attached as Ex. A). The Tunick Affidavit alleges that Mr. Gottesfeld was the user behind an IP address[1] that posted a YouTube video. That video provided publicly available information that unknown others may have used to begin two distributed denial of service ("DDoS")[2] floods. One directed to the servers hosting the Wayside Youth and Family Center in Framingham, Massachusetts ("Wayside") beginning on March 25, 2014, and another directed at servers hosting the Boston Children's Hospital's

---

[1] An IP or "Internet Protocol" address is an address used to identify a computer on a network that uses the Internet Protocol to communicate. These addresses identify the last end-point of a user's connection to a given site or server. In some cases, it identifies an individual computer user. In others, such as when using a proxy or virtual private network ("VPN"), it merely identifies another server used by an unknown user. Unless advanced filtering and detection methods are used, it is trivially easy to "spoof" an IP address, i.e. to send a false address to a server. *See* Spoofing Attack: IP, DNS, & ARP, VERACODE, http://www.veracode.com/security/spoofing-attack (last visited July 1, 2016) (describing IP address spoofing generally).

[2] A DDoS is a method by which multiple computers send a large volume of network traffic to one or more servers. The goal of a DDoS may be to test the servers' traffic capacity or to render those servers unavailable for the time period during which the traffic exceeds the servers' capacity. DDoS floods may be executed by a variety of methods and tools. They may also be executed for a variety of purposes, from standard network testing to political activism to malicious extortion. *See* Denial of Service Attack – Distributed Attack, WIKIPEDIA, https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack (last visited July 1, 2016).

public-facing website beginning on April 19, 2014. *See* Tunick Aff. at pp. 2-5; *see also* Detention Hr'g Tr. at 8:3-5 (identifying the servers as "Boston Children's Hospital computers"). The facts Mr. Tunick alleges to support Mr. Gottesfeld's membership in this conspiracy include:

1) A computer in Mr. Gottesfeld's apartment contained internet browser logs suggesting it was used to create an email address, digitaldruid@riseup.net, (*see* Tunick Aff. at pp. 6-7);
2) A Twitter[3] account, @AnonMercurial2, included the digitaldruid@riseup.net email address in its registration information, (*see id*. at p. 6);
3) The @AnonMercurial2 twitter account called for "attacks on [Wayside]'s website" on March 25, 2014, (*id*.);
4) Also on March 25, 2014, Wayside was the target of a DDoS flood. *(see id* at p. 2; *see also* Detention Hr'g Tr. at 41:17-20 (identifying the "treatment center" as Wayside);
5) Two days earlier, a Twitter account controlled by Mr. Gottesfeld, @stoploganriver, exchanged direct messages with another account, @Digitaghost, where @Digitaghost "told [@stoploganriver] that [@Digitaghost] would be able to successfully attack the [Boston Children's Hospital] servers." (Tunick Aff. at p. 6).

---

[3] Twitter is a social media platform. Users may post up to 140 character public or semi-public posts, or may send private "direct messages" to one another in a one-on-one chat-like feature. As with other social media platforms, messages and public posts vary widely in their seriousness. Posts may be public, or users may "lock" their accounts so that only other accounts they select can read their posts. *See generally* New User FAQs, TWITTER, https://support.twitter.com/articles/13920# (last visited July 1, 2016).

MR. GOTTESFELD'S BACKGROUND

Mr. Gottesfeld is 31 years old, married, and has lived in the Boston area his entire adult life. He has no criminal convictions. Prior to his arrest in this matter, Mr. Gottesfeld worked as a computer security professional at several Boston-area companies. He has, until his arrest and ongoing detention, had a successful career and a stable, supportive family. Before his April 27, 2016 detention hearing, many former employers and family members submitted letters of support to evidence this stable and successful history. (*See* Ex. B). On information and belief, if released, he has a pending employment offer in his area of expertise, namely that his landlord will hire him for website design and software development. He would return to a stable home, living with his wife in Somerville. He is willing to submit to electronic ankle monitoring or the equivalent, and regular check ins with Pretrial and Probation Services. His nephew Greg Brown is prepared to serve as custodian if needed. Other family members are willing to provide bail of $55,000, if the Court requires.

ARGUMENT

There is no good reason to detain Mr. Gottesfeld for a potentially extended period of time pretrial. This is not an alleged crime of violence. This was, if the allegations are true, a political protest in a matter of national interest over the abusive treatment of a young woman detained by Boston Children's Hospital and Wayside against her and her parents will, a young woman who is now suing Boston Children's Hospital. (*See* Detention Hr'g Tr. 41-53; *see also* Michael Levinson, "Parents of Justina Pelletier sue Boston Children's Hospital," BOSTON GLOBE, Feb. 25, 2016, https://www.bostonglobe.com/metro/2016/02/25/parents-justina-pelletier-sue-boston-children-hospital-for-negligence/jCrlgTQBVikJtokEnlFBmN/story.html (last visited July 7, 2016). The government admits this was not "a cyber 9[/]11". (Detention Hr'g Tr. 55:23). The

only real harms alleged, as opposed to breathless speculation, are monetary. (*See* Detention Hr'g Tr. 56:7).

This is a complex CFAA case involving multiple alleged co-conspirators, a large volume of digital forensic evidence, and computers spread across the globe. The volume of evidence will likely take a significant time to analyze in order to properly prepare a defense. The weight of this evidence against Mr. Gottesfeld is unknown at this time as there has been little discovery in this matter. However, based on other CFAA cases, his case will likely require multiple, complex pretrial motions, including motions to suppress and dismiss, should this matter go to trial. During this time, there is no reason that Mr. Gottesfeld should be not be released under appropriate conditions. Otherwise he risks languishing in jail longer than a potential sentence, or needlessly if acquitted. Conditional release under the close supervision of Probation and Pretrial Services eliminates these issues and will reasonably assure Mr. Gottesfeld's appearance in front of the Court.

With the experienced supervision of Probation and Pretrial Services, he will be closely monitored. Given his strong ties to the community, his history of gainful employment, open offers for future employment, and his willingness and ability to engage with Probation and Pretrial Services to comply with his release conditions including electronic ankle monitoring, detention is inappropriate. He poses no danger to the community, and the Government has not disputed this fact.

Conditions Exist That Will Reasonably Assure Mr. Gottesfeld's Appearance in Court

To justify pretrial detention on the basis that Mr. Gottesfeld is a serious flight risk, the government must prove by a preponderance of the evidence that no condition, or combination of conditions, will reasonably assure the defendant's appearance in Court. *See* 18 U.S.C. § 3142 (e);

United States v. Phillips, 732 F. Supp. 255, 259 (D. Mass. 1990); *U.S. v. Martorano*, No. 92-26-J, 1992 WL 73558, at *6 (D. Mass. Mar. 23, 1992). They cannot meet this burden.

To the extent the Government argues Mr. Gottesfeld poses a serious flight risk, their arguments are based Mr. Gottesfeld's actions while his constitutional right to travel was in no way limited or subject to any conditions. *See Shapiro v. Thompson, 394 U.S. 618, 669-70 (1969)* (quoting *Kent v. Dulles*, 357 U.S. 116, 125-26 (1958)) (overruled on other grounds by *Edelman v. Jordan*, 415 U.S. 651, 671 (1974)). This does not show that no release conditions exist that could reasonably assure Mr. Gottesfeld's appearance in court. The First Circuit has recognized for over twenty five years that electronic ankle monitoring, which Mr. Gottesfeld is willing to accept, is an effective means of reasonably assuring a defendant's appearance in court when combined with other conditions, even where that defendant is a serious flight risk. *See United States v. O'Brien*, 895 F.2d 810, 815-16 (1st Cir. 1990).

The government makes no argument that Mr. Gottesfeld poses any danger to the community. As such, electronic ankle monitoring, or the equivalent, combined with the conditions listed below, will reasonably assure Mr. Gottesfeld's appearance in Court.

CONCLUSION

The proposed conditions below are more than sufficient to assure Mr. Gottesfeld's attendance at future appearances and at trial. "In our society liberty is the norm, and detention prior to trial … is the carefully limited exception." *United States v. Salerno*, 481 U.S. 739, 755, 107 S. Ct. 2095, 2105, 95 L. Ed. 2d 697 (1987). Mr. Gottesfeld should be released into the care and support of his family and community, subject to appropriate conditions.

PROPOSAL FOR RELEASE

Mr. Gottesfeld proposes that he be released under the following conditions:

1. Electronic ankle monitoring or the equivalent;
2. Execution of an unsecured appearance bond in the amount of $55,000, signed by Mr. Gottesfeld's family members who have offered to contribute: Greg Brown (nephew), Lisa Brown (sister), and Ben Brown (nephew).
3. Release with custodial supervision by Greg Brown, Mr. Gottesfeld's nephew.
4. Maintaining residence with his wife at 29 Albion Street, Somerville, Massachusetts;
5. Regular telephone check-ins with Pretrial and Probation Services;
6. Reasonable travel restrictions allowing for exceptions with the Court's prior written approval;
7. A no contact order with any alleged victim of the crime and with potential witnesses who may testify concerning the offense;
8. Any other conditions the Court deems appropriate.

Respectfully Submitted,

Dated: July 8, 2016

/s/Tor Ekeland

Tor Ekeland (PHV)
Tor Ekeland, PC
195 Plymouth Street, 5th Floor
Brooklyn, NY 11201
718-737-7264
tor@torekeland.com

Attorney for Defendant Martin Gottesfeld

AFFIDAVIT OF MICHAEL W. TUNICK IN SUPPORT OF AN APPLICATION FOR A COMPLAINT

I, Michael W. Tunick, state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed since 2012. I am currently assigned to the Cyber Crimes Squad of the Boston Field Office of the FBI. As a member of this squad, my responsibilities include investigating criminal offenses including computer intrusions, wire fraud, and conspiracy. Through my training and experience, obtained both prior to and while being employed with the FBI, I am knowledgeable about computer systems, computer networks, networking hardware and software, network security, telecommunication systems, and the means by which individuals use computers, software applications and information networks to commit cyber offenses. During my tenure as a Special Agent, I have participated in the execution of numerous search warrants involving computer equipment, documents, and electronically stored information. Before joining the FBI, I worked in the area of information technology, and computer and network security.

2. Since April 2014, I have been investigating attacks against the computer networks of a large Massachusetts Hospital (the "Massachusetts Hospital" or "Hospital") and a Massachusetts residential treatment center (the "Massachusetts Treatment Center").

3. I submit this affidavit in support of an application for a complaint charging Martin Gottesfeld with conspiracy (18 U.S.C. § 371) to intentionally cause damage to protected computers (18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B)).

4. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses.

"PATIENT A" AND THE NETWORK ATTACKS

5. In early 2014, the press began to report about the case of a teenage girl ("Patient A") who was receiving medical treatment in Massachusetts. As was reported at the time in the press, a Massachusetts state court judge had placed Patient A in the custody of the Massachusetts Department of Children and Families because of concerns that her parents were interfering with her treatment.

6. The issue of Patient A's custody and medical care became a national media story, with religious and political organizations and others asserting that the case was an example of government interference with parental rights.

7. News stories reported that Patient A had been treated at the Massachusetts Hospital, whose doctors continued to oversee her care even after she was transferred, in January 2014, to the Massachusetts Treatment Center.

8. On March 25, 2014, the computer network at the Massachusetts Treatment Center was hit with a Distributed Denial of Service ("DDOS") attack. DDOS attacks direct an enormous amount of network traffic at the target computer server, with the intent to overwhelm that server and disrupt online services. Successful DDOS attacks can take a website or network offline for the duration of the attack, which can range from an hour to days or even weeks.

9. The attack against the Massachusetts Treatment Center lasted for more than a week, crippled the Treatment Center's website during that time, and caused it to spend more than $18,000 on response and mitigation efforts.

10. On March 23, 2014, a video was posted on YouTube calling, in the name of the hacking organization Anonymous, for action against the Massachusetts Hospital in response to its treatment of Patient A. The video, which was narrated by a computer-generated voice, stated

that Anonymous "will punish all those held accountable and will not relent until [Patient A] is free."

11. The YouTube video also stated: "To [The Massachusetts Hospital] – why do you employ people that clearly do not put patients first? We demand that you terminate [physician] from her employment or you too shall feel the full unbridled wrath of Anonymous. Test us and you shall fail." The physician named in the video had been identified in press reports as being involved in the Patient A matter.

12. The YouTube video directed viewers to a posting on the website pastebin.com that contained the information about the Massachusetts Hospital's server necessary to initiate a DDOS attack against that server.

13. On April 19, 2014, the Massachusetts Hospital reported a DDOS attack against the server identified in the pastebin.com posting. The DDOS attack, which directed hostile traffic at the Hospital's network for at least seven days, disrupted that network and took the Hospital's website out of service. The attack also disrupted the Hospital's day-to-day operations as well as the research being done at the Hospital. The Hospital had to re-allocate its resources in a significant way to ensure that patient care was not affected during this period

14. In addition to the DDOS attack, hackers attempted to intrude into the Hospital's network, using malicious e-mail and other means. These attempts were not successful.

15. In an effort to ensure the attack did not compromise patient information, the Hospital decided to shut down the portions of its network that communicated with the internet and its e-mail servers. This effort successfully prevented the attackers from accessing any patient records or other internal Hospital information.

16. This shutdown of the Hospital's website, external internet portal, and e-mail servers, however, impacted the entire Hospital community and particularly the ability of physicians outside of the Hospital to obtain medical records and of patients to communicate with physicians. It also disrupted an important fundraising period for the Hospital by disabling the Hospital's fundraising portal.

17. Responding to, and mitigating, the damage from this DDOS attack cost the Massachusetts Hospital more than $300,000.

THE CONNECTION TO GOTTESFELD

18. I have reviewed Massachusetts Hospital's webserver logs from the time of the DDOS attack. These logs showed hundreds of IP addresses flooding the network with malicious traffic. The IP addresses sending this malicious traffic resolve to geographically dispersed locations. I know that this is consistent with a sophisticated DDOS attack where the perpetrators are masking their physical location.

19. Records for the account that posted the Youtube video calling for the attack on the Hospital show this account is owned and managed by Martin S. Gottesfeld. Those records also show the IP address that was used to post the video on March 23, 2014 and log in to the account on April 1, 2014.

20. Records for RCN, the cable company that controls that IP address, list Martin S. Gottesfeld as the customer assigned to that IP address from at least March 23 to April 1, 2014. RCN records show that Gottesfeld receives his internet service at an address in Somerville, Massachusetts, which is also listed as his residence in Registry of Motor Vehicle records.

21. Based on this and other information, I obtained a search warrant for Gottesfeld's apartment on September 29, 2014.

22. When the FBI executed this search warrant, on October 1, 2014, Gottesfeld agreed to be interviewed. During that interview, Gottesfeld admitted to operating the YouTube account that posted the video calling for the attack on the Massachusetts Hospital and to being the one who posted the video. But he denied participating in any DDOS attacks.

23. During the course of my investigation, I identified a friend of Gottesfeld's, whom I will refer to as Witness 1. I interviewed Witness 1, who told me that he had worked with Gottesfeld on social media projects related to treatment centers that treat children and teenagers like Patient A, although Witness 1 told me that he had no role in the campaign involving Patient A.

24. Witness 1 said that, approximately a week after having read a newspaper article about the DDOS attack against the Massachusetts Hospital, Gottesfeld told him that he (Gottesfeld) had taken down the Hospital's website.[1]

25. Pursuant to the search warrant, I reviewed the computers that Gottesfeld acknowledged were his when I interviewed him at the time of the search. Portions of these computers are encrypted, and I have not yet been able to review them. Other portions are not.

26. I found, in an unencrypted portion of one of Gottesfeld's computers, a series of Twitter direct messages, from March 23, 2014. The messages are between Gottesfeld, using the account "stoploganriver" (which Gottesfeld admitted in the interview was his) and someone using the account "DigitaGhost." One of the message exchanges was:

- Mar 23, 2014 12:49 AM EST @Digitaghost: I was also thinking of attacking one target to show them we are not fucking around. . . .

---

[1] The first time Witness 1 described this conversation with Gottesfeld, he said that it took place during a car ride with Gottesfeld. The second time Witness 1 described it, he said that Gottesfeld discussed the Hospital DDOS attack twice – once during a car ride and once standing outside Gottesfeld's house.

- Mar 23, 2014 12:51 AM EST @Digitaghost: It would require some thought on who #Target first anyway. Vuln scans blah blah blah.

- Mar 23, 2014 12:51 AM EST @Stoploganriver: k, let me run it by the family reps first. I suggest [the Massachusetts Treatment Center].

27. In a later message, DigitaGhost confirmed the Treatment Center's location with Gottesfeld:

- Mar 23, 2014 12:58 AM EST @Digitaghost: This fucking site looks like one of your brainwashing schools.

- Mar 23, 2014 12:59 AM EST @Stoploganriver: It is basically one of those schools, from what we can tell. That's how I was able to bring in #ShutLoganRiver

- Mar 23, 2014 12:59 AM EST @Stoploganriver: that put this in our official purview. . . .

- Mar 23, 2014 1:00 AM EST @Digitaghost: "[city], MA right?"

28. In another exchange that day, Digitaghost told Gottesfeld that he would be able to successfully attack the Treatment Center's servers:

- Mar 23, 2014 1:02 AM EST @Digitaghost: Apache servers left unlatched. Lolololololololol. Fucking #OpSony all over again.

- Mar 23, 2014 1:03 AM EST @Digitaghost: Unpatched*

- Mar 23, 2014 1:04 AM EST @Digitaghost: We can tear that shit up.

29. Two days later, on March 25, 2014, the press reported that the state court judge had granted permanent custody over Patient A to the Massachusetts Department of Children and Families.

30. That day, a Twitter account "@AnonMercurial2" issued a series of public Twitter messages, which included the hashtag #Anonymous, calling for attacks on the Treatment Center's website.

31. Twitter records show that the "@AnonMercurial2" account was created by someone using e-mail account digitaldruid@riseup.net. My review of Gottesfeld's computers

identified internet history logs showing that Gottesfeld created the digitaldruid@riseup.net e-mail address.

GOTTESFELD'S FLIGHT

32. Gottesfeld has been aware of this investigation since the FBI searched his house in October 2014.

33. Last week, I learned that the Somerville Police Department had conducted a wellness check at Gottesfeld's apartment after receiving calls from his employer and from relatives concerned about his whereabouts. According to those calls, he had not been to work, nor had he or his wife had any contact with family members in several weeks, all without explanation. The Somerville Police found nobody home at his house.

34. I also went by his house last Friday but it appeared that there was nobody home and no car was in the driveway.

35. Today, I received a call from an FBI agent in the Bahamas, telling me that Gottesfeld and his wife were on a Disney Cruise Lines ship in the Bahamas. The agent told me that Gottesfeld and his wife were not passengers on the ship but rather had been picked up in a sailboat, not far from Cuba. The sailboat had run into trouble and Gottesfeld and his wife had placed a distress call, to which the cruise ship responded. They had some luggage with them, along with three laptop computers.

36. The cruise ship is scheduled to return to Miami tomorrow morning, February 17, 2016.

THE STATUTES

37. The conspiracy statute makes it a crime for: "two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency

thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy." 18 U.S.C. § 371.

38. The computer fraud and abuse act makes it a crime to: "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A).

39. The statute defines a "protected computer" to include one used in or affecting interstate or foreign commerce or communication 18 U.S.C.A. § 1030(e). The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Here, the DDOS attacks impaired the availability of the victims' computer systems by taking them off-line at times. The § 1030 violation becomes a felony if (among other things) it causes the potential modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals. § 1030(c)(4)(B).

CONCLUSION

40. Based on the information described above, I have probable cause to believe that Martin Gottesfeld committed the crime of conspiracy, in violation of 18 U.S.C. § 371.

Sworn to under the pains and penalties of perjury,

Michael W. Tunick
Special Agent, FBI

Subscribed and sworn to before me on February 16, 2016.

Hon. David H. Hennessy
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA Plaintiff, v. MARTIN GOTTESFELD, Defendant.	Case No.: 16-MJ-4117 (MBB)

CERTIFICATE OF SERVICE

TOR EKELAND, an attorney duly admitted to practice before this Court and not a party to the above-captioned action, hereby affirms the following to be true, under penalty of perjury:

1. I am over 18 years of age and am the managing partner of Tor Ekeland, P.C. and counsel for Mr. Gottesfeld.
2. On Friday, July 8, 2016, I filed a true and correct copy of the above motion via ECF, causing it to be served electronically on counsel for the United States of America.
3. I certify that a true copy of the above documents were served on the attorney of record for the United States of America by electronic mail on Friday, July 8, 2016.

Date: July 8, 2016

By: */s/ Tor Ekeland*

Tor Ekeland
Tor Ekeland, PC
195 Plymouth Street, Fifth Floor
Brooklyn, New York 11201-1044
T: 718-737-7264
F: 718-504-5417
Email: tor@torekeland.com