UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	No.: 16-cr-10305-NMG
	)	
MARTIN GOTTESFELD,	)	
	)	
Defendant.	)	

GOVERNMENT'S SENTENCING MEMORANDUM

In 2014, Martin Gottesfeld launched successive and sustained cyberattacks on the computer networks of Wayside Youth & Family Support Network and the Boston Children's Hospital. These attacks put the lives of children at risk. Yet Gottesfeld remains unrepentant. He claims he committed no crime at all. He has obstructed justice by destroying evidence. And he has shown his contempt for the rule of law and for this Court at every stage of this proceeding.

To punish Gottesfeld for his crimes, to protect the public from the continuing danger he poses, and to deter others from committing dangerous and costly network attacks under the guise of "activism," the government recommends a sentence of 150 months' incarceration, followed by three years of supervised release in which Gottesfeld's use of electronic devices would be subject to reasonable restrictions and monitoring. The Court should also order Gottesfeld to pay restitution in the amounts of $425,159 and $17,771 to Boston Children's Hospital and Wayside Youth & Family Support Network, respectively.

In support of this sentencing memorandum, the government incorporates by reference two supplemental filings: 1) the Government's First Submission in Support of Sentencing of Martin Gottesfeld, filed under seal on January 4, 2019 ("Gov't First Submission"); 2) the Government's Second Submission in Support of Sentencing of Martin Gottesfeld, also filed on

January 4, 2019 ("Gov't Second Submission"). Each of these filings includes an affidavit from FBI Special Agent Michael W. Tunick attaching several exhibits. The government further relies on and incorporates the testimony and exhibits from the trial of Martin Gottesfeld.

I. The Offense Conduct

In early 2014, Martin Gottesfeld, a computer engineer, became fixated on a custody case involving a Connecticut teenager named Justina Pelletier. The case had garnered considerable interest in the press and was controversial. Pelletier had been admitted to Boston Children's Hospital ("Children's Hospital") in early 2013. According to media reports, Pelletier had been previously diagnosed with mitochondrial disease. Also according to media reports, doctors at Children's Hospital believed that she actually suffered from a psychological disorder and were concerned that Pelletier's parents were contributing to her condition. After this dispute arose over her diagnosis, the Massachusetts Department of Children & Families ("DCF") sought and obtained temporary custody of Pelletier through the Massachusetts Juvenile Court. The proceeding involved a Juvenile Court Judge taking evidence consisting of, among other things, "extensive psychiatric and medical testimony" and "voluminous psychiatric and medical records." Ultimately, based on "clear and convincing evidence," the Juvenile Court found that Pelletier needed the care and protection of the Commonwealth. PSR ¶¶ 19-21.

Gottesfeld never met Justina Pelletier or her family. He had no contact with Pelletier's lawyers, her family's lawyers, or her court-appointed guardian ad litem. He had no communication with her doctors. He had no access to her medical records. PSR ¶ 21. Instead, he relied on television news and talk shows, social media, and other internet-based sources to, in his words, "vet" the Pelletier case. As Gottesfeld told a reporter in a recorded jail call, he had "taken a lot of time—over a day—and looked at the Pelletier case and similar cases, and looked

at that kind of the overall methodology that was being used in the Pelletier case at BCH, and I found it to be very wanting. To be very … to be distinctly unscientific." *See* Gov't Second Submission, Tunick Aff., Ex. 17 (9/30/2016, 10:31 a.m.).

Gottesfeld concluded based on his day-long review that the diagnosis of doctors at Children's Hospital was incorrect and that Pelletier in fact suffered from mitochondrial disease—the original diagnosis from another hospital. He further concluded that DCF was wrong to take custody of Justina, and that the agency had filed misleading affidavits with the Juvenile Court in support of its effort to obtain custody. According to Gottesfeld, Children's Hospital was intentionally torturing Justina Pelletier to death, in violation of state and federal law, and the United Nations Convention Against Torture. To this day, he maintains that the hospital doctors intentionally maimed and tortured Pelletier. PSR ¶ 21.

Gottesfeld identifies himself as a member of Anonymous—a loosely knit, international group of hackers. Upon drawing his conclusions about the Pelletier case, Gottesfeld issued a "distress call" to other members of Anonymous, calling on them to focus on the Pelletier matter and to assist him in securing her discharge from Children's Hospital. PSR ¶ 25, n.2; Gov't Second Submission, Tunick Aff., Ex. 17 (9/30/2016, 10:31 a.m. & 4:05 p.m.).

Pelletier was discharged from Boston Children's Hospital in January 2014.[1] However, she remained in DCF custody and was living at the Framingham campus of the Wayside Youth and Family Support Network ("Wayside"), a nonprofit that provides a range of psychiatric and

[1] She had been ready to be discharged seven months earlier, but according to the Juvenile Court, DCF's efforts to find a suitable placement for Pelletier were hampered by her parents. Specifically, the Juvenile Court and DCF tried to place Pelletier in a program appropriate to her needs 20 minutes from her Connecticut home. The program declined to accept Pelletier after her father told the program he would sue if Pelletier were placed there. The Juvenile Court found that other programs also refused to accept Pelletier for fear of litigation. PSR ¶ 20.

family support services to children, young adults, and families in Massachusetts. PSR ¶ 23.

A. March 20, 2018 Statement on Behalf of Anonymous ("the Pastebin Post")

On March 20, 2014, while Pelletier remained at Wayside, Anonymous posted a statement on the website pastebin.com threatening retaliation against Children's Hospital if it did not fire a doctor reportedly involved in Pelletier's care and "return" her to her parents, despite the fact that Pelletier had been discharged from Children's Hospital months before and was in DCF custody and living at Wayside. The Pastebin Post announced the launch of the Anonymous "Operation Justina" or "OpJustina." Gottesfeld promoted this announcement on social media. PSR ¶ 24.

The Pastebin Post claimed that Pelletier was being physically and mentally tortured and declared: "We will punish all those held accountable and will not relent until Justina is Free." Gottesfeld testified that the statement was issued on behalf of Anonymous and was written by an unidentified co-conspirator who used the Twitter handle @digitaghost ("Digitaghost"). Anonymous accused the state court judge handling Pelletier's matter of "abduct[ing] children away from their parent's [sic] with impunity," and stated, "Anonymous is here to remind you who is in charge of this country and as a result we feel that you should be exposed from behind your veil of secrecy and deceit." Anonymous posted the judge's name, address, and telephone number and called on "the American people . . . to use this information to your maximum potential in order to save Justina. Call his home and demand answers, mail letters to his home telling him that you will not stand for this attack upon the innocent . . . ." PSR ¶ 25.

In the Pastebin Post, Anonymous also "doxed" (*i.e.*, posted the name, home address, home phone, work phone number and work fax number of) a Boston Children's Hospital doctor

reportedly involved in Pelletier's care.[2] Anonymous demanded that Children's Hospital "terminate Alice W. Newton from her employment or you to [sic] shall feel the full unbridled wrath of Anonymous. Test us and you shall fail. . . . This will be your first and final warning. Failure to comply will result in retaliation which you will not be able to withstand." The Pastebin Post then provided information about the IP address of the public-facing website of Boston Children's Hospital, and the type of software the web server was running. This IP address was among the targets at which Gottesfeld later directed his DDOS attacks. PSR ¶ 26.

B. Preparation for Attack on Wayside's Computer Network

On March 22 and March 23, 2014, Gottesfeld and "Digitaghost" exchanged a series of private Twitter messages. They discussed their expectation that the state court judge would soon make a final decision regarding Pelletier's custody. They stated that they hoped the judge would return Pelletier to her parents' custody, but they planned to attack if the judge did not do so. PSR ¶28.

Gottesfeld had conducted no research regarding Wayside, other than looking at its website. He spoke to no current or former residents or current or former staff members. He never visited the Wayside Framingham campus, where Pelletier resided. Nonetheless, he concluded that Wayside was a "brainwashing" school that he believed was another part of what he called the "troubled teen industry"—institutions that treat teens with serious emotional, psychological, and medical problems, but in Gottesfeld's view, abuse these children. Gottesfeld had begun advocating against schools he deemed part of the "troubled teen industry." PSR ¶ 29. He pressured them via social media to shut down or change their policies, and if they did not, he

[2] Gottesfeld admitted in recorded jail calls with a reporter that he "doxed" another physician—a neurologist—involved in Pelletier's care.

attacked their networks. As Gottesfeld told a reporter from jail, "Wayside looked like, and really is, a troubled teen industry facility in Massachusetts. It's not as bad as the one in Utah, but you know some very disturbing stuff still happened to Justina at Wayside, and the [Children's Hospital] was still pulling the strings." Gov't Second Submission, Tunick Affid., Ex. 17 (9/30/16, 4:05 p.m.).

On March 25, 2014, the Juvenile Court awarded permanent custody of Justina Pelletier to DCF, agreeing with the assessments of Massachusetts DCF, Connecticut DCF, and a court-appointed guardian ad litem that "conditional custody of [Justina Pelletier's] parents is not in her best interest at this time." The Court's Disposition Order, Trial Exhibit 94, was subject to review and redetermination in June 2014. The Disposition Order was issued under seal, but was leaked to the Boston Globe. The online edition of the Boston Globe posted a link to the opinion in a March 25, 2014 article that Gottesfeld accessed from his personal computer. Nonetheless, Gottesfeld did not bother to read the opinion, and instead relied on news reporting and social media postings about the case. PSR ¶ 30.

Hours after the Juvenile Court's decision became public, Gottesfeld and Digitaghost launched a DDOS attack on Wayside's computer network. As Wayside responded to the network attack, Gottesfeld changed his tactics in order to continue to disrupt the computer network. PSR ¶ 32.

Gottesfeld engaged in what he described as a "cat and mouse" game with Wayside. Among the tools he used, for example, was "Tor's Hammer"—a DDOS script that executes a particular type of DDOS attack. When Wayside successfully mitigated that type of attack, Gottesfeld moved onto a different attack method. Gottesfeld attacked the network for several weeks. Gottesfeld tweeted about his exploits and the progress of his attack from his

AnonMercurial account. PSR¶ 32.

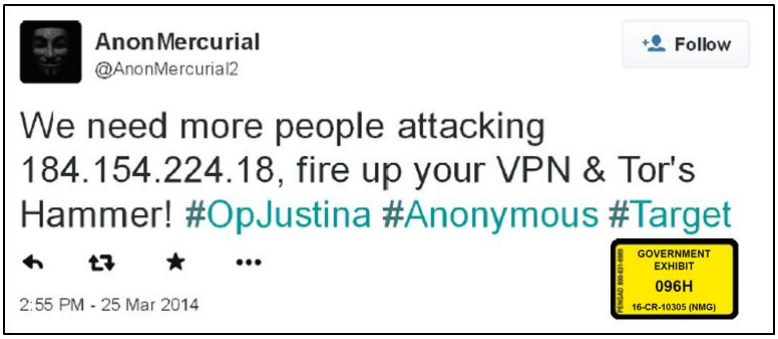

Figure 1: Gottesfeld's March 25, 2014 Tweet. VPN and Tor's hammer are tools that Gottesfeld encouraged others to use to join in his DDOS attack on Wayside's website.

Figure 2: Gottesfeld's April 1, 2014 Tweet publicizing his takedown of www.waysideyouth.org.

Gottesfeld's DDOS attacks disabled Wayside's website, its e-mail network, and its access to its residents' electronic health records. The attack impaired Wayside's ability to communicate with medical providers, staff, families, and DCF over e-mail; the staff's ability to access Wayside's internal network, where it kept residents' records; and the public's ability to obtain information from Wayside's public-facing internet page, www.waysideyouth.org. Wayside spent approximately $17,771 defending itself against the attack. PSR ¶ 37.

The purpose of Gottesfeld's attack was to increase political pressure on Wayside to refuse to provide services to Pelletier, possibly resulting in her placement at another facility. PSR ¶ 38.

B. Gottesfeld and Co-conspirators Attack the Boston Children's Hospital Computer Network

While attacking the Wayside computer network, Gottesfeld began preparing to attack the Children's Hospital computer network. He recognized that the Children's Hospital network was robust and well-funded—in his words, a "much more difficult target" than the Wayside network. In early April 2014, Gottesfeld began probing the Children's Hospital network and testing ways to disrupt it. Many of his early efforts were not successful. He was also aware that Digitaghost had attempted to disrupt the network, but testified that "the methods that [Digitaghost] was attempting and the bandwidth available to him would have been like shooting a pea shooter at a tank." For about two weeks, Gottesfeld tested various attack methods. Gottesfeld testified that during this period, "I would try something; it would either work or it wouldn't. If it worked temporarily, they would try to adapt, and then I would counter-adapt." Gottesfeld again referred to this as the "cat-and-mouse" game he had previously played with the team defending the Wayside network. PSR ¶ 40.

Ultimately, Gottesfeld determined that he needed to create an entire botnet of compromised computers in order to direct enough traffic at the Children's Hospital network to knock the hospital off the internet. He re-wrote an existing piece of malware—the "moon worm"—that he then used to infect approximately 40,000 computer routers. He controlled those infected routers from his personal computer. On April 13, 2014, in the middle of the night, Gottesfeld began a series of test runs, directing his botnet to flood the Children's Hospital network with internet traffic. This was the beginning of Gottesfeld's successful DDOS attack on the hospital network. He began by sending about twice the normal weekday traffic to the IP address of one of the hospital's public facing websites—the same IP address referenced in the

Anonymous internet post and in the video that Gottesfeld posted on YouTube on March 23. This was just the first phase of his attack. In a self-published article after his arrest, Gottesfeld wrote: "I coded around the clock for two weeks to perfect the attack. Small test runs were made. BCH bragged to the media that they were withstanding the onslaught and hadn't been taken down. They had no idea what was to come." PSR ¶ 40; Trial Exhibit 35.

Indeed, Children's Hospital struggled to maintain internet connectivity during these early days of Gottesfeld's DDOS. The volume of internet traffic directed at the Children's Hospital network from April 11 to April 20, 2014 is depicted below:

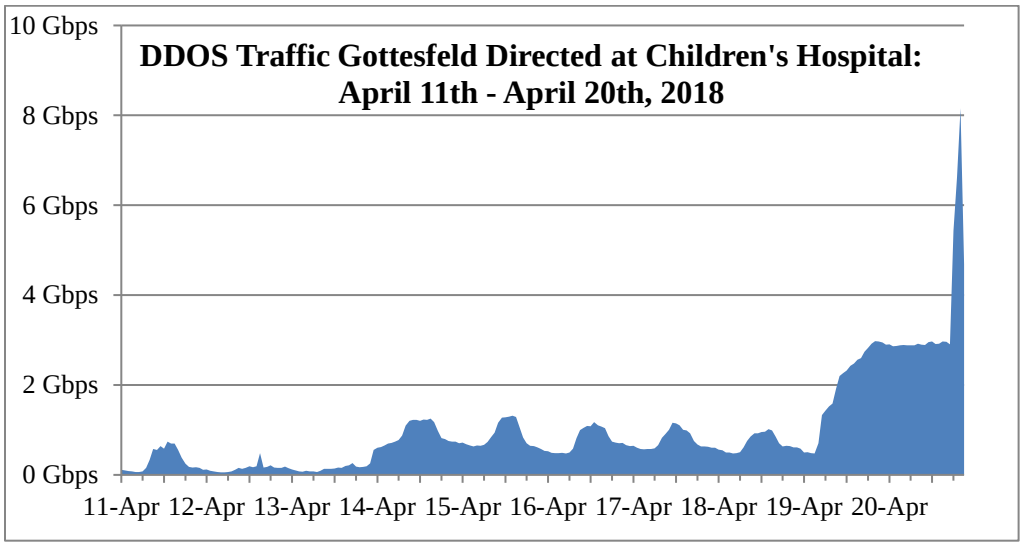

Figure 3: Network traffic directed at Children's Hospital, as set forth in Gov't Ex. 5A.

The hospital's technology staff worked around the clock to defend the network during this period, but Gottesfeld continued to adjust his attack methods. As a result, doctors, nurses, and staff had trouble accessing the internet-based tools they used to care for their patients. Access to critical applications was slow or intermittent. The Children's Hospital formulary was among the critical applications affected by Gottesfeld's DDOS attack. The formulary serves as the backbone for the administration of medicines in any hospital. At Children's Hospital, the

formulary is particularly complex, covering some 2,500 medications, and is highly customized to meet the needs of its pediatric patients (including custom dosing instructions and other critical information). The formulary is also primarily internet-based. During the first wave of Gottesfeld's DDOS attack, access to the formulary was slow, and inconsistent. Dr. Al Patterson testified that the hospital had to invoke emergency procedures and distribute printed copies of archived editions of the formulary to strategic locations throughout the hospital. Even then, electronic dosing information remained unavailable. PSR ¶ 42.

Similarly, access to the application UptoDate was intermittent and slow during the first wave of Gottesfeld's DDOS attack. UptoDate is a detailed, internet-based compendium of disease state information that doctors and nurses rely upon extensively. It and the formulary are among the most frequently accessed applications at the hospital. PSR ¶ 43.

Gottesfeld's network attack also affected the hospital's ability to process prescriptions, including the hospital's ability to route prescriptions electronically to pharmacies in the community and throughout the country. The hospital had to resort to paper prescriptions and faxing documents in order to ensure that outpatients were able to receive critical medications. As the internet outages and slowdowns were intermittent during this phase of Gottesfeld's attack, there were substantial resources devoted to ensuring that electronic orders were in fact completed (and did not remain electronically queued in the various applications), and that when electronic orders were not available, paper or other alternative means were used. A pharmacy relations employee at the hospital testified that she had no way to confirm whether prescriptions for the hospital's cystic fibrosis patients were being rejected. She was unable to do her job, which was to get medications into the hands of these critically ill patients, because she was unable to send or receive faxes or emails. . PSR ¶¶ 44-45.

On April 19, 2014, Gottesfeld taunted the hospital from his AnonMercurial Twitter account. Under the banner of #Anonymous, he threatened to post personal information about Children's Hospital staff ("d0xes"). He further threatened to breach the network and to access confidential patient records, which the hospital was required to protect under federal law, including under the Health Insurance Portability and Accountability Act ("HIPAA"). PSR ¶ 46.

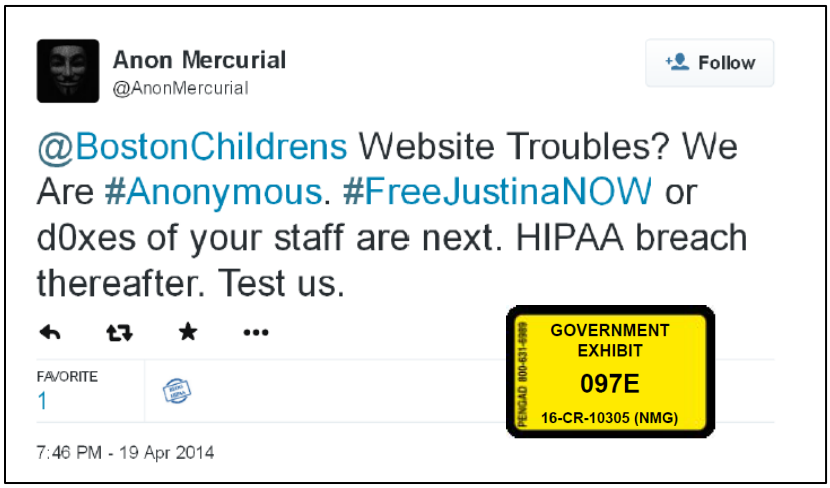

Figure 4: Gottesfeld's April 19, 2014 Tweet threatening to breach the Children's Hospital network and exfiltrate patient medical records and staff personal information.

Around the time of this Tweet, Gottesfeld caused a massive surge in traffic to the Children's Hospital network, completely overwhelming it, and knocking the entire hospital off the internet. All internet connected services were disrupted, including the critical resources described above, such as the hospital formulary, UptoDate, and the electronic prescription system. Moreover, patient medical records could not be accessed from outside the hospital. Research data could not be sent or received. In short, the hospital was cut off from the internet. Gottesfeld understood that his attack would knock the entire hospital off the internet based on his research into the network architecture. PSR ¶ 47.

Gottesfeld also understood, based on the network architecture that the hospital used, that

his attack would affect the internet connections of several other hospitals and medical facilities in the Longwood Medical Area. He acknowledged at trial that internet traffic to approximately 65,000 IP addresses on the same subnet as Children's Hospital would also be affected by his attack. The institutions served by these IP addresses and affected by the attack included the Dana Farber Cancer Center; Beth Israel Hospital; Jocelyn Diabetes Center; Brigham & Women's Hospital; and the Harvard School of Public Health, and the Harvard Medical School, among others. PSR ¶ 48.

Gottesfeld claims he had no involvement in or prior knowledge of efforts to breach the network and steal medical records and staff information. But his contemporaneous statements during the attack show this is false. His April 19th Tweet immediately preceded and correctly predicted a massive effort to penetrate the network through spearfishing and malicious emails; SQL injection attacks; and cross-site scripting attacks. Gottesfeld acknowledged at trial that these attacks were conducted by members of Anonymous, and that he personally brought Anonymous into the Pelletier matter by launching #OpJustina. His Tweets established that he was involved in and publicized OpJustina. Gottesfeld also testified he was aware that a specific group of hackers separate from him and DigitaGhost were involved in attempting to breach the network. Witnesses who worked for Children's Hospital and from the cybersecurity company Radware testified that DDOS attacks like Gottesfeld's are frequently used to disguise malicious traffic that can be slipped into a network amidst an overwhelming volume of junk data. Gottesfeld's Tweet was an important factor in Children's Hospital's decision to take down portions of the network to protect the network from penetration by Gottesfeld and Anonymous. One Children's Hospital witness noted: "[I]t was a constant game of guessing what's going to happen next and being on guard to figure out . . . you know, given the Anonymous reputation

and their reputed level of skill, where they might find a breach to come in. It's much easier to attack the network than it is to defend the network. PSR ¶ 49.

The IT staff at Children's Hospital was not able to bring the hospital back online, as Gottesfeld continued to escalate the DDOS attack beginning April 19, 2014. On April 20, 2014—Easter Sunday and the day before the Boston Marathon—the hospital hired Radware, which specializes in DDOS mitigation, on an emergency basis to divert all internet traffic directed at the hospital to a data center in Israel, where Gottesfeld's attack traffic, including the malicious traffic of his co-conspirators, was filtered out from legitimate internet traffic, and the hospital's internet connectivity was restored. Radware's initial engagement, made necessary by Gottesfeld's attacks, cost Children's Hospital approximately $120,000. PSR ¶ 50.

Gottesfeld continued to escalate the DDOS through April 24, 2014, when DDOS traffic peaked at nearly 28 gigabits per second—at the time according to witnesses, one of the largest DDOS attacks ever conducted, in terms of traffic volume. By way of comparison, the connection between the firewall protecting the Children's Hospital network and the router connecting it to the internet (i.e., the total internet bandwidth for the hospital) allowed for a no more than two gigabits per second of traffic. Below is a graph depicting the total volume of traffic directed at Children's Hospital (filtered attack traffic is indicated in red):

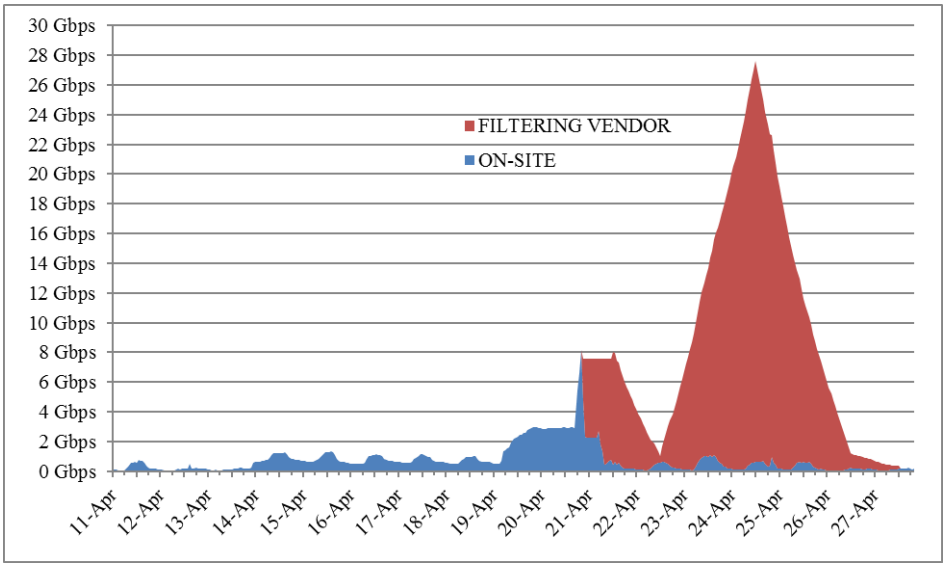

Figure 5: Chart depicting internet traffic directed at the Children's Hospital Network based on Children's Hospital records.

At the peak of the attack on April 24, 2014, Gottesfeld Tweeted:

Figure 6: Gottesfeld's April 24, 2014 Tweet stating his intention to reduce the volume of DDOS traffic, but promising to attack again until Pelletier was returned to her parents' custody.

As depicted in Figure 5: Chart depicting internet traffic directed at the Children's Hospital Network based on Children's Hospital records., Gottesfeld reduced traffic following this Tweet. But he threatened to resume the attack until Pelletier was returned to her parent's custody—a decision that Children's Hospital did not control. The hospital administration therefore continued to

prepare for additional network attacks and to enlist services of cybersecurity firms to prepare for and defend against them. Moreover, Gottesfeld had brought Anonymous into his campaign, and testified that there were members of OpJustina conducting other types of attacks than the DDOS. PSR ¶ 53.

In the midst of Gottesfeld's DDOS attack and his threats to breach the network, the hospital took its public-facing website down, disabled websites that patients and providers used to access hospital records and services, and disabled its email network (so as to be able to scan for emails containing viruses). As noted, the attack overwhelmed the resources of the hospital's IT staff, requiring it to retain consultants and other service providers such as Radware, both to mitigate the increased network traffic caused by the DDOS attack, to assess whether attackers had in fact penetrated its network (as Gottesfeld promised), and to defend against the ongoing efforts that followed Gottesfeld's threats. These resources cost the hospital hundreds of thousands of dollars. PSR ¶ 54.

The attacks substantially disrupted the hospital's normal operations, requiring its staff to use manual procedures and other workarounds, both to communicate and to access resources related to patient care. For example, a leading pulmonologist at the hospital testified to the interdisciplinary care that the hospital provides to a very vulnerable population of lung transplant patients. She described a distressing inability to communicate with her colleagues over email, and to receive communications from her patients' hometown doctors about their care. PSR ¶ 55.

Gottesfeld sought to inflict maximum financial impact on the hospital. He planned his attack to disrupt the Hospital's ability to raise money during a key fundraising period. He launched the attack on the eve of a holiday weekend that culminated in Patriot's Day and the running of the Boston Marathon, one year after the marathon bombing. As Gottesfeld stated to a

reporter in an October 1, 2016 jail call:

> My goal was basically to demonstrate a point that to the ruthless who only care about money, if money is all you care about, fine. This will cost you money. If money is more important to you than this girl's life. If money is more important to you than this girl's life, fine, we'll hit you in your pocketbook.

PSR ¶ 56.

The hospital spent approximately $425,000 defending and mitigating the network attacks of Gottesfeld and his coconspirators and implementing measures to better defend the network against the imminent attacks that Gottesfeld and his co-conspirators promised to carry out on behalf of Anonymous. The hospital also lost approximately $328,000 in charitable donations because of the disruption to its fundraising efforts, as Gottesfeld stated was his intention. PSR ¶ 57.

C. Gottesfeld's DDOS Attacks on Institutions Related to His Pelletier Campaign

Gottesfeld launched DDOS attacks against other institutions based on his belief that they were affiliated with Children's Hospital or that they failed to support his cause. For example he DDOSed the utility company NSTAR for providing utility services to the Boston Children's Hospital. PSR ¶ 59.

Figure 7: Gottesfeld's April 21, 2014 Tweet at @NSTAR_News.

Gottesfeld also DDOSed the Massachusetts Medical Society—the statewide professional association for physicians and medical students. At trial, he could not recall what the Massachusetts Medical Society was or why he DDOSed it. His contemporaneous Tweet establishes that he DDOSed the entity because it did not sufficiently support his view of the Pelletier matter. PSR ¶ 61.

Figure 8: Gottesfeld's April 21, 2014 Tweet at @MassMedical.

As part of #OpJustina, Gottesfeld and DigitaGhost also DDOSed Framingham.com (and Tweeted a link to the Pastebin Post calling for doxing and attacks on Children's Hospital and its employees). PSR ¶ 63.

D. Gottesfeld Began Attacking Targets Using the Name "Packet Signal"

After the Boston Children's attack, and over the summer of 2014, Gottesfeld continued his DDOS campaign against other institutions that he believed were complicit in the troubled teen industry. Gottesfeld used a new Twitter handle, @PacketSignal, to Tweet at and taunt the victims, just as he had with AnonMercurial and AnonMerucial2. Gottesfeld used similar language, phrasing, capitalization, and punctuation, and presented statistics from uptimestatistics.com as proof of his successful DDOS attacks. PSR ¶ 65.

For example, in September 2014, under the banner of OpLiberation, referenced in his message board in Gov't Ex. 44, Gottesfeld attacked the website of the National Association of Therapeutic Schools and Programs ("NATSAP"):

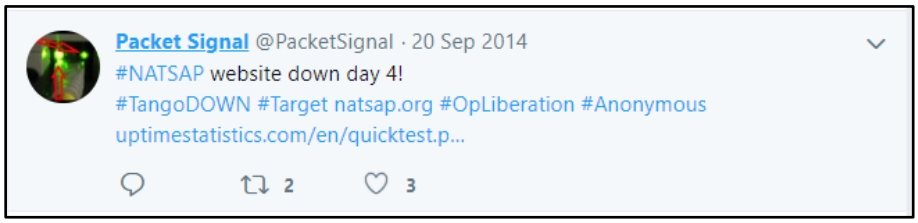

Figure 9: Gottesfeld Tweeting as Packet Signal about his attack on www.natsap.org.

He also DDOSed GreatSchools.org (a non-profit website that provides ratings and other school-related information), Sorenson's Ranch School in Utah, and the Judge Rottenberg Educational Center, a special needs day and residential school located in Canton, Massachusetts. PSR ¶ 66-70.

II. Sentencing Guidelines

The U.S. Probation Office correctly determined that Gottesfeld's advisory sentencing guideline range is 121 to151 months' incarceration based upon a Total Adjusted Offense Level of 32 and a Criminal History Category of I (PSR ¶¶ 97,101). The Probation Office determined Gottesfeld's offense level as follows: (1) a base offense level of 6, given the offense of conviction; (2) a 14-level enhancement pursuant to USSG§ 2B1.1(b)(1)(H) because Gottesfeld caused losses of more than $550,000 but not more than $1.5 million; (3) a two-level enhancement pursuant to USSG § 2B1.1(b)(2)(A)(i) because the offense involved 10 or more victims; (4) a two-level enhancement pursuant to USSG § 2B1.1(b)(10)(C) because Gottesfeld used sophisticated means to carry out the offense; (5) a two-level enhancement pursuant to USSG § 2B1.1(b)(19)(A)(iii) because Gottesfeld's attacks caused a substantial disruption of critical infrastructure (specifically, a hospital network); and (6) a two-point adjustment for

obstruction of justice pursuant to USSG § 3C1.1. PSR ¶¶ 86-97.

Gottesfeld has objected to all of the enhancements except the two points for disruption of critical infrastructure. PSR at pp. 45-46 & 50 (Objections 14-17, & 28-29). The evidence at trial, however, along with the supplemental findings made by the Probation Office amply support each of the enhancements set forth in the PSR.

A. Gottesfeld's Cyberattacks Caused More than $1 Million in Loss

Gottesfeld engaged in a campaign to terrorize the Boston Children's Hospital, claiming that its physicians were maiming and torturing a patient in their care. His stated purpose was to inflict as much financial damage on Children's Hospital as he could. Indeed, as he later wrote in the Huffington Post, he timed his attack to coincide with a major fundraising period for the hospital, and successfully knocked the fundraising portal offline. He now challenges the calculation of the losses he caused, claiming the hospital suffered no more than $150,000 in losses. *See* PSR pp. 45 & 46. His claim is unavailing.

The Sentencing Guidelines provide that "[i]n the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service." USSG § 2B1.1 Cmt., n.3(A)(v)(III).[3]

[3] The Guidelines definition of loss incorporates the statutory language from 18 U.S.C. § 1030(e)(11). Defendant cites two cases suggesting that all loss must stem directly from an "interruption of service," but ignores persuasive caselaw to the contrary. *See Gen. Linen Serv., Inc. v. Gen. Linen Serv. Co.*, No. 12-CV-111-LM, 2015 WL 6158888, at *4 (D.N.H. Oct. 20, 2015) (describing breadth of CFAA definition of loss and expressly holding that loss is not limited to costs arising out of an interruption of service).

As described above, Children's Hospital could not respond to the scale and scope of Gottesfeld's attack without emergency assistance from outside vendors. One witness characterized the approximately 28 gigabit-per-second attack in 2014 as unprecedented. As a result, the hospital hired Radware on an emergency basis to siphon off Gottesfeld's attack traffic and allow legitimate internet traffic to flow again, restoring internet-based resources that were vital to the care and treatment of its patients. Children's Hospital similarly required the services of Mandiant, RSA, Guidepoint, and other vendors to determine whether a breach of the network occurred (as Gottesfeld had publicly threatened from his Anonymous Twitter account); to identify vulnerabilities that could be exploited during Gottesfeld's attack; to monitor for additional attack traffic and network breach attempts; and to supplement its own staffing to accomplish these goals. *See* First Govt' Submission, Tunick Affid., Ex. 5. These costs alone totaled approximately $425,159 and fall well within the definition of "loss" under USSG § 2B1.1 and 18 U.S.C. § 1030(e)(11), as they constitute reasonable costs incurred "responding to an offense," "conducting a damage assessment," and "restoring the data, program, system, or information to its condition prior to the offense." Indeed, the estimate is conservative, as it does not include the countless hours that Children's Hospital's own information technology staff spent responding to Gottesfeld's attack. PSR ¶ 42, 58. *See generally United States v. Millot*, 433 F.3d 1057, 1061 (8th Cir. 2006); *United States v. Middleton*, 231 F.3d 1207, 1213-14 (9th Cir. 2000) ("There is no basis to believe that Congress intended the element of 'damage' to depend on a victim's choice whether to use hourly employees, outside contractors, or salaried employees to repair the same level of harm to a protected computer.")

Of course, the damage Gottesfeld caused went beyond the costs of defending against his network attacks. Gottesfeld intentionally struck the hospital's computer network and its

fundraising portal during a significant fundraising campaign near the one-year anniversary of the 2013 Boston Marathon bombings. BCH estimates that the attack cost approximately $328,000 in lost donations, which also qualifies as "loss" under § 1030(e)(11) (i.e., "revenue lost"). PSR ¶ 75. Gottesfeld disputes the total, questioning whether the baseline assumptions underlying the hospital's calculation are accurate, and also whether Children's Hospital could have brought its fundraising systems back online sooner. He offers no support for these assertions, however.

In any case, the Guidelines make clear that the Court need not establish loss with precision, but rather, may make a reasonable estimate of the loss, based on the available information." *United States v. Cox*, 851 F.3d 113, 125 (1st Cir. 2017); *see* USSG 2B1.1 App. Note. 3. The estimate here is reasonable, and in any case, even a small fraction lost donations would result in a loss amount greater than $550,000, which is all that is required to support the 14-point enhancement at issue. This fact is significant because Gottesfeld's DDOS attack on Children's Hospital caused losses at other institutions as well. Harvard spent $204,000 in response to Gottesfeld's attack; Wayside spent $17,771; the Joselin Diabetes Center spent $1,000. PSR ¶ 75. Thus, the Court could substantially discount the losses incurred by these entities, and the total would still far exceed the threshold for the 14-point enhancement, even without addressing other victims of Gottesfeld's uncharged conduct.

Gottesfeld's principal attack on this calculation is that he should not be held accountable for any payments of lost donations that occurred after April 24, 2014, when he claims to have stopped his attack, and further that he should not be held accountable for any actions taken to protect the network against non-DDOS attack methods. In substance, Gottesfeld now wishes to insulate himself from the that actions of the people whom he recruited to attack Children's

Hospital—actions he was aware of at the time and which he publicly stated through his Anonymous Twitter account were part of his "OpJustina" campaign. The law does not allow him to do so.

Under the Guidelines, Gottesfeld is responsible for the acts of others in connection with his attacks on the Children's Hospital and Wayside computer networks if those acts were: (1) within the scope of the jointly undertaken criminal activity; (2) in furtherance of that criminal activity, and (3) reasonably foreseeable in connection with that criminal activity. USSG § 1B1.3(a)(1)(B). The evidence at trial established that Gottesfeld is the one who spearheaded the campaign against Wayside and Children's Hospital. He sought and obtained assistance from other members of Anonymous. He was aware of the attempts to breach the Children's Hospital Network by his fellow "Anons." And he of course publicly Tweeted at the hospital that he was a part of this effort by threatening on April 19, 2014, to breach the hospital's network to obtain the personal information of Children's Hospital staff and to obtain protected healthcare information of the hospital's patients. Gottesfeld publicly stated that he was part of the effort not only to knock the network offline through his DDOS, but to breach the network. In his words: "We Are #Anonymous. #FreeJustinaNOW or d0xes of your staff are next. HIPAA breach thereafter. Test us." That Tweet immediately preceded a flood of malicious traffic designed to penetrate the protected hospital computers.

Moreover, multiple witnesses, including from Children's Hospital and Radware, testified at trial the DDOS attacks like the one Gottesfeld perpetrated are often conducted in concert with efforts to penetrate a network using malware. This evidence, and the reasonable inferences the Court can draw from it, are sufficient to conclude by a preponderance of the evidence that Gottesfeld should be held accountable not only for the massive DDOS attack the he perpetrated,

but also for the reasonably foreseeable attacks that the handful of Anonymous sympathizers he recruited perpetrated on his behalf and in furtherance of his criminal activity. The hospital's costs in responding to Gottesfeld's attacks were necessary and reasonable, especially in light of his credible threats to continue them well into the future unless Children's Hospital did his bidding.

B. Gottesfeld's Cyberattacks Involved Ten or More Victims

There were at least four unique victims who suffered financial losses as a result of the charged conduct: Wayside, Children's Hospital, Joslin Diabetes Center, and Harvard University. PSR ¶ 75. Under USSG § 2B1.1, however, a defendant's offense level "is increased both on the basis of the conduct for which he was convicted and on the basis of the 'relevant conduct' for which he is found responsible by a preponderance of the evidence." *United States v. Cox,* 851 F.3d 113, 121 (1st Cir. 2017). Such conduct need not be charged, but must be related to the offense of conviction. *United States v. Gonzalez,* 857 F.3d 46, 58 (1st Cir. 2017) ("[t]he Guidelines were not intended to discontinue the courts' historical practice of considering the relevant circumstances of the defendant's real conduct, whether those circumstances were specifically charged or not."

Under the Guidelines, uncharged offenses are sufficiently related to the offense of conviction if they are part of the same course of conduct or a common scheme or plan as the offense of conviction. *See* USSG § 1B1.3(a)(2). These concepts are "closely related." For two or more offenses to constitute a common scheme or plan, "they must be substantially connected to each other by at least one common factor, such as common victims, common accomplices, common purpose, or similar *modus operandi*." *Id*. at cmt. n. 5(B)(i) (emphasis supplied).

Here, Gottesfeld himself testified that the DDOS attacks on Children's Hospital and Wayside were part of a unified, ongoing campaign against what he called the "troubled teen industry." He similarly told a Rolling Stone reporter in a recorded jail call that he saw Wayside and Children's Hospital as part of the "troubled teen industry":

> I kind of rallied the troubled teen industry troops that we had that we had been working with. Because at that point, Justina was already out of [Children's Hospital], and at Wayside, and Wayside looked like, and really is, a troubled teen industry facility in Massachusetts.

See Second Gov't Submission, Tunick Affid., Ex. 17 (9/30/2016, 4:05 p.m.).

As a part of his campaign, Gottesfeld launched numerous DDOS attacks against several institutions in addition to Wayside and Children's Hospital, including Logan River Academy (PSR ¶¶ 9-36), Sorenson's Ranch School (PSR ¶¶ 71-72), and the Judge Rottenberg Educational Center (PSR ¶¶ 73-74). These were all institutions that he claimed were mistreating children in some manner. He also attacked businesses or associations that provided services for or were otherwise related to these institutions, including BestNotes (PSR ¶¶ 17-18), Great Schools (PSR ¶¶ 66-68), the National Association of Therapeutic Schools and Programs (PSR ¶¶ 69-70), and the Massachusetts Medical Society (PSR ¶¶ 61-62).[4]

The evidence at trial made clear that, as misguided as Gottesfeld's theory was, he viewed all of his victims as part of the same "troubled teen industry." Gottesfeld told DigitaGhost by Twitter message that he "brought in #ShutLoganRiver" to the Pelletier controversy because Wayside was, as DigitaGhost put it, "one of [Gottesfeld's] fucking brainwashing schools." [Trial Exh. 42 at 4]. Gottesfeld used the same type of attacks as he had used against Wayside

[4] There were DDOS attacks on other entities—such as the utility company NSTAR and the website www.framingham.com—that did not suffer financial loss and therefore did not qualify as "victims" under the Guidelines. PSR ¶¶ 59-60 (NSTAR) & 63-64 (www.framingham.com). These attacks nonetheless provide further evidence of a common scheme.

and Children's Hospital against his other targets — launching DDOS attacks directed at public-facing websites. He then mocked his victims over social media, using his signature taunts "TangoDOWN" and "Website Troubles?," and citing uptimestatistics.com to demonstrate the effectiveness of his attacks. They were the same techniques, whether he was attacking Logan River Academy, Children's Hospital, or NATSAP.

Figure 10: Gottesfeld's March 24, 2014 Tweet announcing his takedown of the Logan River Academy website.

Figure 11: Gottesfeld Tweeting as Packet Signal about his attack on www.natsap.org.

These attacks all occurred between the spring and early fall of 2014—a relatively compressed timeframe that immediately preceded and followed the attacks on Wayside and Children's Hospital. There is therefore sufficient evidence to show that the attacks on each of the above-described victims shared a common purpose and similar modus operandi and therefore constitute relevant conduct.

They were also part of a course of conduct, connected closely enough as to "warrant the conclusion that they are part of a single "spree or ongoing series of offenses." *See* USSG § 1B1.3, cmt. n. 5(B)(ii). Each of the factors that the Sentencing Commission evaluates to determine whether offenses are sufficiently connected to be part of the same course of conduct within the meaning of USSG § 1B1.3 is present here: Gottesfeld's attacks were similar to one another; were repeated regularly, and took place at close intervals to each other. *See United States v. Eisom*, 585 F.3d 552, 557 (1st Cir. 2009) ("A district court's determination of the scope of a particular scheme, plan, or course of conduct 'represents a practical, real-world assessment of probabilities, based on the totality of proven circumstances.'") (quoting *United States v. Sklar*, 920 F.2d 107, 111 (1st Cir.1990)).

The total number victims of the offense is accordingly ten or greater, and the two-point enhancement under USSG 2B1.1(b)(2)(A)(1) applies. *See generally United States v. Cox*, 851 F.3d 113, 124 (1st Cir. 2017) (applying enhancement for 10 or more victims based on uncharged relevant conduct).

C. Gottesfeld's Used Sophisticated Means to Conduct His Cyberattacks

The guidelines define "sophisticated means" as "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense" USSG § 2B1.1 cmt. n. 9(B). That Gottesfeld used sophisticated means to attack his targets is manifest. He used tools to hide identity and location, such as a virtual machine, virtual private networks and the Internet-anonymizing browser, TOR (i.e., "the Onion Router"). More significantly, he re-wrote an existing piece of malware—the "moon worm"—that he then used to infect approximately 40,000 computer routers around the world, and he controlled those infected routers from his personal computer in Somerville, both disguising his identity and location, and

marshalling the resources of that hijacked computer network equipment to bombard Children's Hospital with enough traffic to knock the hospital off the internet. Courts have approved the sophisticated-means enhancement in the context of CFAA cases involving considerably less complex circumstances than these. *See, e.g.*, *United States v. Musacchio*, 590 F. App'x 359, 366–67 (5th Cir. 2014), aff'd, 136 S. Ct. 709, 193 L. Ed. 2d 639 (2016) (use of administrator accounts to read employee emails and forwarding the text of the emails to webmail accounts "to avoid leaving records" constituted sophisticated means).

Gottesfeld objects that he described the method of his attack on Children's Hospital on cross examination, and that this testimony was somehow protected by a proffer letter he signed while attempting to negotiate a plea with the government in 2015. He offers no support for this claim. The defendant's sworn testimony at trial in his affirmative case is—of course—appropriate for the court to consider at sentencing and accordingly the two-point enhancement under USSG § 2b1.1(B)(10)(c) is appropriate here.

D. By Knocking Boston Children's Hospital Off the Internet and Affecting the Communications of Multiple Area Medical Facilities, Gottesfeld Caused a Substantial Disruption of Critical Infrastructure.

Under USSG § 2B1.1(b)(19)(A)(iii), a 6-point enhancement applies if the defendant's crime caused a substantial disruption to "critical infrastructure." The plain text of the guideline and associated commentary support the Probation Office's application of this enhancement.

The Guidelines define "critical infrastructure" as "systems and assets vital to national defense, national security, economic security, *public health or safety*, or any combination of those matters." USSC § 2B1.1, cmt. n. 15(A) (emphasis supplied). The critical infrastructure may be publicly or privately owned, and may include "emergency services (including medical, police, fire, and rescue services)." Children's Hospital is a not-for-profit, comprehensive center

for pediatric health care and is one of the largest pediatric medical centers in the United States. Children's Hospital conducts approximately 25,000 inpatient procedures and almost receives almost 600,000 ambulatory visits each year. Doctors at Children's Hospital perform annually about 26,000 surgeries. While the hospital serves as a regional community organization, treating local patients with widely varying medical needs, Children's Hospital is also an international destination patients with highly complex medical conditions that can be treated at few other, if any, institutions in the world. PSR ¶ 39. The testimony at trial demonstrated aspects of the emergency services the hospital provides, and accordingly, the hospital should be considered an asset "vital . . . to public health and safety." *Cf. United States v. Mitra*, 405 F.3d 492, 496-97 (7th Cir. 2005) (disruption of city's emergency radio system used by first responders, among others, fit within scope of "emergency services.")

There is little case law interpreting this Guidelines provision in closely analogous circumstances, however, and the government acknowledges there is contrary authority. Specifically, in *United States v. Brown*, 884 F.3d 281 (5th Cir. 2018), the Fifth Circuit assessed the text, commentary, and underlying related statutory basis for the guideline and concluded that for a disruption to be "substantial," it must have the potential to be national in scope. *Id*. at 287. In short, application of this enhancement would be a closer call under a novel theory.

Should the Court determine that the 6-point enhancement under USSG § 2B1.1(b)(19)(A)(iii) does *not* apply, a 4-point enhancement under § 2B1.1(b)(19)(A)(ii) would apply instead, as the defendant was convicted of an offense under 18 U.S.C. § 1030(a)(5)(A).

In any case, for the reasons described in Part III below, the two-point difference between these provisions should not affect the sentence imposed, based on the totality of the circumstances, and all of the sentencing factors identified in 18 U.S.C. § 3553(a).

E. Gottesfeld Obstructed Justice By Destroying Evidence of His Attacks

Gottesfeld admitted that following the attack on Children's Hospital and before the execution of a search warrant at his Somerville home, he destroyed substantial evidence of his attack by irrevocably deleting a virtual machine named "Druid." The government's forensic expert testified that the commands Gottesfeld ran were the equivalent of running digital evidence through a shredder, three times.

Gottesfeld objects to the application of a two-point enhancement for obstruction of justice under USSG § 3C1.1 because, in his view, "the described destruction of evidence did not meaningfully interfere with law enforcement's investigation in the context of the entire case." PSR p. 50. Gottesfeld misstates the law. The standard is not whether destruction of evidence did in fact interfere with law enforcement's investigation, but whether the evidence "could have influenced or affected the official investigation." *United States v. Feldman*, 83 F.3d 9, 13 (1st Cir. 1996). The "test for materiality under the obstruction-of-justice guideline is not stringent." *Id.* Clearly, the destruction of data on the very device used to perpetuate the crime had the ability to influence or affect law enforcement's investigation, and the two-point obstruction enhancement is therefore appropriate.[5]

[5] The government does not seek an obstruction enhancement based on Gottesfeld's flight to Cuba, which is analogous to "avoiding or fleeing from arrest," a ground that the Sentencing Commission has described as conduct to which USSG § 3C1.1 does not apply. That being said, the court should consider his flight to Cuba under section 3553(a). He should not be permitted to perpetuate the false narrative that he was a persecuted human rights activist – a narrative that the Cuban authorities rejected. In reality, he was on the run from the consequences of his criminal conduct.

III. Sentencing Guidelines & Recommendation

The government respectfully recommends, however it analyzes the Guidelines in dispute, that the Court sentence Gottesfeld to 150 months' incarceration and three years' supervised release.

To this day, Gottesfeld has refused to acknowledge that his actions were criminal and that he put lives and patient care in danger at Wayside and Children's Hospital. He continues to lash out at any one who disagrees with his worldview, characterizing them as corrupt, conflicted, incompetent, or deceitful. That includes each attorney that has represented him, any judicial officer who has issued an unfavorable ruling in his case or Justina Pelletier's juvenile court matter, and the entire prosecution team. Gottesfeld's recent 86-page affidavit all but promises that he will re-offend while wearing the cloak of "activism" or "independent journalism." He is the rare first-time offender who poses such a serious risk of recidivism.

Witness after witness testified to overwhelming evidence of his guilt and proved just how dangerous and disruptive his criminal acts were. Gottesfeld's was not a "show trial" or a "dog and pony" show, as he claimed on social media. His complete lack of respect for the rule of law only reinforces the risk that he will re-offend in a dangerous and costly way.

Rather than come to terms with his actions, he has continued to spin self-published conspiracy theories that attempt to excuse his criminal conduct. This is a defendant who accused a sitting federal judge of falsifying a court document because it had typographical error in it. It is this same pattern of acting out based on unsubstantiated conclusions that led him to attack the victims in this case. It is terrifying to contemplate the next cause Gottesfeld will take up and the means by which he hold others accountable for perceived injustices.

There are too many dark corners of the internet where conspiracy theories flourish. The Court's sentence in this case needs to deter other inhabitants of those dark corners from turning digital harm into real-world consequence. A member of this Court, in imposing a 17.5 year sentence on a serial cyber-stalker, recently responded to the defendant's claim that his crimes were less serious because they were entirely digital:

> [I]n today's world, that does not diminish the crimes in any way. In fact, it ought to bring home to all of us how interconnected we are and what havoc can be wreaked by the improper evil criminal conduct in which you so gleefully engaged.

United States v. Lin, 18-CR-10092 (D. Mass. Oct. 3, 2018) (WGY). These words apply with considerable force to Gottesfeld's actions — using his technical skills to weaponize the internet and wreak havoc from behind a keyboard — and the need for this Court's sentence to reflect the seriousness of that offense.

The United States accordingly respectfully requests that the Court sentence defendant Martin Gottesfeld to 150 months in the custody of the Bureau of Prisons, with three years' supervised release to follow. Given the circumstances of Gottesfeld's conviction, there should be reasonable restrictions placed on his use of the internet and electronic devices upon his release.

Respectfully submitted,

Andrew E. Lelling
United States Attorney

By: */s/ David J. D'Addio*
David J. D'Addio
Seth B. Kosto
Assistant U.S. Attorneys

January 4, 2019

CERTIFICATE OF SERVICE

I hereby certify that this document, the Government Sentencing Memorandum, will be sent via U.S. mail to Martin Gottesfeld, Inmate ID #71225, at the Plymouth County Correctional Facility, 26 Long Pond Road, Plymouth, MA 02360, which is the address from which his most recent pro se correspondence has been sent.

/s/ David J.D'Addio

Dated: January 4, 2019