



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA

S2 12 Cr. 185 (LAP)

- v. -

JEREMY HAMMOND,

a/k/a “Anarchaos,”

a/k/a “sup_g,”

a/k/a “burn,”

a/k/a “yohoho,”

a/k/a “POW,”

a/k/a “tylerknowsthis,”

a/k/a “crediblethreat,”

a/k/a “ghost,” and

a/k/a “anarchacker,”

Defendant.

**GOVERNMENT’S MEMORANDUM OF LAW
WITH RESPECT TO SENTENCING**

PREET BHARARA
United States Attorney for the
Southern District of New York

Attorney for the United States
of America

THOMAS BROWN
ROSEMARY NIDIRY
Assistant United States Attorneys
Of Counsel

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

S2 12 Cr. 185 (LAP)

- v. -

JEREMY HAMMOND,
a/k/a “Anarchaos,”
a/k/a “sup_g,”
a/k/a “burn,”
a/k/a “yohoho,”
a/k/a “POW,”
a/k/a “tylerknowsthis,”
a/k/a “crediblethreat,”
a/k/a “ghost,” and
a/k/a “anarchacker,”

Defendant.

The Government respectfully submits this memorandum in advance of the sentencing of Jeremy Hammond (“Hammond” or the “defendant”), which is scheduled for November 15, 2013 at 10:00 a.m. In his plea agreement with the Government (the “Plea Agreement”), Hammond has stipulated that the applicable United States Sentencing Guidelines (“Guidelines” or “U.S.S.G.”) range would be 151 to 188 months’ imprisonment but, in light of the statutory maximum of the offense of conviction, that his Guidelines sentence is 120 months’ imprisonment. In its Presentence Investigation Report (“PSR”), the United States Probation Office (“Probation Office”), consistent with the Plea Agreement, recommends a sentence of 120 months.

Contrary to the picture he paints of himself in his sentencing submission, Hammond is a computer hacking recidivist who, following a federal conviction for computer hacking, went on to engage in a massive hacking spree during which he caused harm to numerous businesses,

individuals, and governments, resulting in losses of between \$1 million and \$2.5 million, and threatened the safety of the public at large, especially law enforcement officers and their families.

For the reasons set forth below, given the nature and circumstances of Hammond's outrageous and widespread cyber attacks, his history and characteristics, including the fact that he committed the instant offense conduct after having been previously convicted of closely similar criminal hacking, and the need to promote respect for the law and ensure just punishment, the Government submits that a stipulated Guidelines sentence of 120 months is entirely appropriate in this case.

BACKGROUND

I. Hammond's Offense Conduct

Hammond was a prolific and technically skilled hacker who launched cyber attacks against scores of governmental institutions, law enforcement organizations, and businesses during a nearly year-long rampage. Hammond's aim was to break into victims' computer systems, steal data, deface websites, destroy files and dump online the sensitive personal and financial information of thousands of individuals – all with the object of creating, in Hammond's own words, maximum "mayhem." (*See, e.g.*, Bates # 63161-62, 63172.) Between June 2011 and March 2012, when he was identified and arrested, Hammond attacked computer networks belonging to victims around the world. Evidence of Hammond's hacking spree came from online chats recorded by a cooperating witness (the "CW"), in which Hammond described his computer attacks; from victims; and from Hammond's laptop, which he was using at the moment

of his arrest to hack into at least one victim's computer network and which contained a trove of electronic files that not only corroborated several of the hacks he described to his co-conspirators and the CW, but also revealed that Hammond had engaged in many more attacks than previously known.

A. The Arizona Department of Public Safety Hack¹

In June 2011—just weeks after Hammond's term of supervised release had ended on May 20, 2011, following his two-year term of imprisonment for a conviction on a federal computer hacking charge (PSR ¶¶ 60-63) – Hammond contacted the CW, who was a member of the Anonymous-affiliated hacking group LulzSec. In the preceding months, members of LulzSec had hacked into the computer systems of a number of governmental and business organizations around the world and had publicly dumped online stolen data in a series of high-profile “press releases,” generating significant press attention. In subsequent conversations with the CW, Hammond said that he had stolen a large number of confidential law enforcement documents from the Arizona Department of Public Safety (“AZDPS”), including training manuals, private emails, and other sensitive data; provided samples of these documents; and sought LulzSec's assistance in publicly releasing the full set of stolen data in a similarly high profile manner.² (Bates # 78130-64.) Hammond told the CW that “black hats [criminal hackers]

¹ In the Plea Agreement, Hammond admitted the Arizona Department of Public Safety hack as relevant conduct to be considered at the time of his sentencing. (Plea Agreement at 1.)

² Upon learning that AZDPS's computer systems had been compromised, the FBI immediately notified AZDPS, as it did each time it received notice that Hammond or his co-conspirators had compromised an entity's computer systems.

need to unite especially going against police and the government,”³ that he had a “three punch knockout plan” to dump the information on the Internet, and that he would write at least the first press release. (Bates # 78162, 78185, 78218, 78240.)

On June 23, 2011, members of LulzSec, including Mustafa al Bassam, a/k/a “Tflow” and Jake Davis, a/k/a “Topiary,” publicized “Chinga La Migra [Fuck the Border Police] Bulletin #1,” LulzSec’s public release of numerous sensitive law enforcement documents that Hammond had stolen from AZDPS computer servers, along with the personal details of Arizona law enforcement officers – and their spouses – including names, email accounts and passwords, home addresses, cell phone numbers, and home phone numbers. (*See, e.g.*, Bates # 78197, 78199, 78213-14, 78246-47.) Over the next two weeks, “Operation Anti-Security” or “AntiSec,” a new Anonymous-affiliated group that succeeded LulzSec, completed Hammond’s “three punch knockout plan” by releasing “Chinga La Migra II” and “Chinga La Migra III,” each of which contained additional sensitive Arizona law enforcement data and law enforcement officers’ personal information, including information stolen from computer systems used by the Arizona Fraternal Order of Police.⁴

³ The text of the chats is reproduced here as it appears in the chat logs; errors in spelling and punctuation have not been corrected.

⁴ Indeed, the following note was found on Hammond’s laptop: “[the Arizona Fraternal Order of Police’s website] <-- we already owned 6 months ago but we can own again for lulz.” Significantly, at least one core member of LulzSec was profoundly disturbed by the invasiveness and purposelessness of Hammond’s attack on AZDPS and online dump of confidential and sensitive law enforcement data and personal information about police officers and their families. In an interview with the BBC in May 2013 following his conviction and sentence in the United Kingdom on charges related to his LulzSec activities, Jake Davis confessed that the “Chinga La Migra” data dump on June 23, 2011 was a “turning point” for him: “I thought this hack [of

B. The Stratfor, California Statewide Law Enforcement Association, New York State Association of Chiefs of Police and Special Forces Gear Hacks⁵

In December 2011, Hammond took over, organized and led a cyber attack against Strategic Forecasting, Inc. (“Stratfor”), a private intelligence firm based in Texas. During the course of that attack, Hammond (1) stole at least 200 gigabytes⁶ of confidential information from Stratfor’s computer systems, including the content of Stratfor employees’ emails, account information relating to approximately 860,000 Stratfor clients, approximately 60,000 credit cards numbers belonging to Stratfor clients, and internal Stratfor corporate documents, including company financial data; (2) caused that information to be publicly disclosed; (3) defaced the Stratfor website; and (4) deleted all of the data on Stratfor’s computer servers, effectively destroying the company. (PSR ¶ 15.) Hammond’s criminal associates made at least \$700,000 worth of unauthorized charges using the credit card information stolen and distributed by Hammond. (PSR ¶ 28.)

Hammond first learned about Stratfor from the CW on December 5, 2011. The CW told Hammond that another hacker, who used the online alias “hyrriiya,” had said he had hacked the

AZDPS] has gone way too far – there’s no point to this thing. It’s just harming police officers . . . This doesn’t entertain anybody or help anybody anywhere.” *See* <http://www.bbc.co.uk/news/technology-22526021>.

⁵ As described *infra*, Hammond pleaded guilty before Your Honor to the Stratfor hack. In the Plea Agreement, Hammond also admitted to the Special Forces Gear hack (among others) and agreed that it could be considered as relevant conduct at the time of his sentencing. (Plea Agreement at 2.) He did not admit the California Statewide Law Enforcement Association or New York State Association of Chiefs of Police hacks at his guilty plea.

⁶ A gigabyte is a measure of data storage equivalent to approximately 675,000 pages of text.

(Bates # 63167.)

In further online conversations with his criminal associates, Hammond assumed leadership of how the hack would be exploited. For example, in a chat on December 19, 2011, Hammond admonished his co-conspirators that while they should make as many unauthorized charges to the stolen Stratfor subscribers' credit cards as possible to create "financial mayhem," deleting data and dumping sensitive stolen information on the Internet were just as important:

[Hammond] those ccs [credit cards] and financial mayhem is definitely the most lulzy and newsworthy element of this attack

[Hammond] and also goes with the lulzmas theme of stealing from rich and giving to poor

[Hammond] an equally important part is destroying their servers and dumping their user/address list and private emails

[Hammond] with the goal of destroying the target

[Hammond] I'm hoping bankruptcy, collapse

(Bates # 63172.)

Hammond also took charge of how the destruction of Stratfor and the public disclosure of the data he had stolen would be publicized for maximum impact. Among other things,

Hammond:

- created the code that defaced Stratfor's website prior to the deletion of all of the data on Stratfor's computer network (Bates # 63197-98, 63202);
- arranged for "teasers" of limited amounts of stolen data – principally Stratfor subscribers' personal information and credit card numbers – to be published online to generate interest in the main dump of information that Hammond had planned (Bates # 63164, 63191);

- drafted “press releases” to go along with each disclosure (Bates # 63166, 63192, 63194);
- directed his co-conspirators to examine the stolen Stratfor material for information about famous or noteworthy Stratfor subscribers that could be singled out for public ridicule (Bates # 63215); and
- came up with the idea of sending spam emails to thousands of Stratfor subscribers purporting to come from a Stratfor executive and attaching a document (a “zine”) that not only documented the Stratfor hack, but also contained sensitive information, including data on thousands of emails and credit cards, that Hammond had stolen as a result of cyber attacks on the websites and computer systems of three other law enforcement targets: the California Statewide Law Enforcement Association; the New York State Association of Chiefs of Police; and Special Forces Gear, a company which sold equipment to military and law enforcement personnel.⁹ The document also included a claim that more than \$500,000 in unauthorized charges had been made to credit cards stolen through the hacking activity. (Bates # 63166, 63170, 63202-03, 63271, 77637 *et seq.*)

On December 24, 2011, after causing his co-conspirators to hype the event on Twitter (Bates # 63205 (“Can we get them twitters going, hypin people up?”)), Hammond defaced Stratfor’s website and, minutes later, deleted all of the data on its computer servers – knocking Stratfor offline for the next six weeks. (Bates # 63197-99, 63205-09.) Unsurprisingly, given

⁹ In a chat with a co-conspirator on December 13, 2011, Hammond had boasted of hacking into Special Forces Gear’s website and stealing emails and customers’ credit card numbers and discussed the impact of including that stolen data in the “zine,” particularly because it contained personal information relating to a federal law enforcement agent:

[Hammond]	I re-owned and rooted their server
[Hammond]	and grabbed the encryption keys back again . . . as well as their massive mail spools
<~elChe>	lol
[Hammond]	dropping the CCs [credit cards] will only enhance the mayhem
[Hammond]	especially cause we got an FBI home address + card

(Bates # 63162.)

Hammond's efforts to publicize the hack, reaction in the press and online was immediate. When a Stratfor subscriber expressed outrage on a social media site, Hammond located among the Stratfor data he had stolen the subscriber's personal information, including the subscriber's credit card data, email address and home address; pasted it in a chat channel visible to his co-conspirators; noted that the credit card information was still good; and directed his co-conspirators to make fraudulent charges against it. (Bates # 63229-31 ("Yall can go ahead and ride on him.")) Finally, on December 29, after having published several teasers of stolen data, Hammond dumped online account information relating to approximately 860,000 Stratfor subscribers, as well as approximately 60,000 credit cards numbers belonging to Stratfor clients. On January 6, 2012, Hammond caused the spam email attaching the zine noted above to be sent to Stratfor clients, whose information, including email accounts, he had compromised.

C. Hammond's Other Online Attacks

Hammond's recorded online chats with the CW, evidence recovered from his laptop at the time of his arrest, and his admissions in the Plea Agreement show that Hammond has engaged in many more attempted and successful online attacks. In his Plea Agreement, Hammond admitted that, in addition to the AZDPS and the Special Forces Gear hacks noted above, in 2011 and 2012 he also attacked, stole and disseminated confidential information from websites and computer networks used by the following victims:

- the Federal Bureau of Investigation's Virtual Academy;
- Brooks-Jeffrey Marketing, Inc. ("BJM"), which maintained various law enforcement-related websites;
- Vanguard Defense Industries ("Vanguard");

- the Jefferson County, Alabama Sheriff's Office;
- the Boston Police Patrolmen's Association ("BPPA"); and
- Combined Systems, Inc.

(PSR ¶¶ 30-37.)

In addition to the foregoing, in recorded chats with the CW, Hammond bragged about attacks against the computer systems and websites of over 30 businesses, governments, and law enforcement organizations, including, among others, the Syracuse Police Department; the town of Gates, New York; "OnGuardOnline.gov," a federal website designed to promote safe, secure and responsible use of the Internet; the Lake County, Florida Sheriff's Office; and the Boston Police Department.

Hammond's laptop, which was seized at the time of his arrest while he was chatting online with the CW, also contained a wealth of evidence relating to his criminal hacking activities. Among other things, Hammond's laptop contained files that documented attacks on computer systems belonging to scores of entities, including successful cyber attacks against:

- the Federal Trade Commission and its website, as well as at least two other related consumer protection websites operated by the federal government;
- the New York Police Department's Equipment Section, including the theft of a database containing the names, home addresses, email accounts and credit card information of at least hundreds of customers of its website;
- Southern Police Equipment Supply, including its website;
- the Austin Police Retirement System, including the theft of a database containing the names, email addresses, passwords, dates of birth, and associated account numbers of at least hundreds of retired police officers; and
- Panda Security and its website, including the theft of email addresses and passwords of hundreds of Panda Security employees and users.

Indeed, an examination of Hammond's laptop revealed open terminal panels which showed that Hammond was logged into Panda Security's computer network at the very moment he was arrested.¹⁰ Other open files on Hammond's desktop included, for example, .pdfs of tax returns belonging to innocent third parties, lists of usernames and passwords for various victim websites and servers, and an email application which showed that Hammond had live access to numerous victim email accounts that he had compromised.¹¹

II. Hammond's Arrest and Indictment

On March 5, 2012, agents of the Federal Bureau of Investigation ("FBI") arrested Hammond at his residence in Chicago on an arrest warrant issued pursuant to a complaint, 12 Mag. 611, that had been filed in the Southern District of New York. The Complaint charged Hammond with conspiracy to commit computer hacking, in violation of Title 18, United States Code, Section 1030(b) (Count One); substantive computer hacking, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), (c)(4)(B)(i) and 2 (Count Two); and conspiracy to commit access device fraud, in violation of Title 18, United States Code, Section 1029(b)(2) (Count Three).

On May 2, 2012, Superseding Indictment S1 12 Cr. 185 (LAP) was filed in the Southern District of New York. In addition to the charges in the Complaint, which all related to

¹⁰ On March 7, 2012, unknown individuals – likely Hammond's criminal associates with whom he had shared his successful hack of Panda Security – defaced its website and announced that it had been hacked in retaliation for Hammond and his LulzSec co-conspirators' arrests two days before. *See, e.g.*, <http://www.foxnews.com/tech/2012/03/07/anonymous-retaliates-for-lulzsec-arrests-hacks-panda-security-website/>.

¹¹ (Bates # 1500-1555.)

Hammond's participation in the Stratfor hack, the Superseding Indictment charged Hammond with an additional count of conspiracy to commit computer hacking for his involvement in the AZDPS hack with other members of LulzSec, in violation of Title 18, United States Code, Section 1030(b),¹² and one count of aggravated identity theft in violation of Title 18, United States Code, Section 1028A, in connection with the Stratfor hack.

III. Hammond's Guilty Plea and the Presentence Investigation Report

On May 28, 2013, Hammond pleaded guilty before Your Honor to a superseding information, S2 12 Cr. 185 (LAP), pursuant to a plea agreement with the Government. The Superseding Information, which was filed on the same day, charged Hammond with one count of conspiracy to engage in computer hacking, after having been previously convicted of federal computer hacking charges, in violation of Title 18, United States Code, Section 1030(b), in connection with Hammond's participation in the Stratfor hack.

According to the terms of the Plea Agreement, Hammond admitted to participating in eight other cyber attacks besides the Stratfor hack and stipulated that this additional criminal activity was relevant conduct to be considered by the Court at the time of his sentencing.¹³ (Plea

¹² The Superseding Indictment also included a separate conspiracy to commit computer hacking charge against Ryan Ackroyd, Jake Davis, Darren Martyn, and Donncha O'Cearrbhail for their involvement in a group called Internet Feds, a precursor hacking group to LulzSec. Ackroyd, Davis and Martyn were also charged along with Hammond for the LulzSec conspiracy; and Ackroyd, Davis, Martyn, and O'Cearrbhail were also charged along with Hammond for the Stratfor hack with AntiSec.

¹³ The eight additional hacks to which Hammond admitted participating in were each the subject of a separate FBI investigation. As a result of Hammond's admission of those hacks as relevant conduct, the Government agreed not to charge Hammond for those separate offenses. In addition, the Government agreed not to charge Hammond further based on evidence obtained

Agreement at 2-3.) Hammond stipulated that his total adjusted Guidelines offense level was 31, including enhancements based on (1) a loss of more than \$1,000,000 but less than \$2,500,000; (2) 250 or more victims; (3) the fact that Hammond's offense conduct involved sophisticated means; (4) the fact that Hammond's offense conduct involved an intent to obtain personal information or the unauthorized public dissemination of personal information; and (5) the fact that Hammond's offense conduct involved a computer system used by or for a government entity in furtherance of the administration of justice. (*Id.* at 3-4.) In addition, Hammond stipulated that he is in Criminal History Category IV, based in part on his conviction, in 2006 in the Northern District of Illinois, for a violation of Title 18, United States Code, Title 1030(a)(2) (computer hacking), which arose from his cyber attack on and theft of thousands of credit cards from a victim's computer system and resulted in a sentence of 24 months' incarceration to be followed by a term of three years' supervised release; and because he committed the instant offense while on probation following his conviction in 2010 in Cook County (IL) Circuit Court for mob action. (*Id.* at 4-5.) Hammond agreed that his stipulated Guidelines sentence was 120 months. (*Id.* at 6.) Finally, Hammond also agreed that neither a downward nor an upward departure from the stipulated Guidelines sentence was warranted. (*Id.*)

In the PSR, the Probation Office concurred with the offense level calculations and sentencing range agreed to by Hammond in the Plea Agreement, and recommended a term of incarceration of 120 months. (PSR ¶¶ 42-77, 111; page 28.)

from the laptop computer seized at the time of his arrest, or based on evidence obtained from his communications with the CW. (Plea Agreement at 2-3.)

ARGUMENT

A sentence of 120 months is warranted in this case. Hammond is a hacking recidivist who, over the course of almost a year, launched cyber attacks that harmed businesses, individuals, and governments; caused losses of between \$1 million and \$2.5 million; affected thousands of people; and threatened the safety of the public and of law enforcement officers and their families. In 2006, Hammond was sentenced to a term of 24 months' incarceration on a federal computer hacking charge. Undaunted by this prior conviction and sentence, shortly after completing his term of supervised release for it and while on probation for yet another conviction, Hammond began a sustained campaign during which he executed cyber attacks against the websites and computer networks of scores of victims. Hammond's history of recidivism and complete disregard for the law belies his current claim at sentencing that he will not re-engage in this same criminal conduct upon his release from prison. Moreover, Hammond's own statements prior to his arrest show that, contrary to his contentions now, Hammond was motivated by a malicious and callous contempt for those with whom he disagreed, particularly anyone remotely related to law enforcement, not a "concern[] with both transparency and privacy." (Def. Mem. at 33.) For all of these reasons, as well as for the importance of deterrence, promoting respect for the law, and providing just punishment in this case, the Government respectfully submits that a sentence of 120 months would be sufficient, but not greater than necessary, to serve the legitimate purposes of sentencing.

I. Applicable Law

As the Court is well aware, in determining Hammond's sentence, the Court must consider the factors set forth in 18 U.S.C. § 3553(a). The Court must also impose a sentence sufficient, but not greater than necessary, to comply with the purposes set forth in paragraph (2) above. *Id.*

The Sentencing Guidelines, which "should be the starting point and the initial benchmark" for sentencing, *Gall v. United States*, 128 S.Ct. 586, 596 (2007), take into account in a case such as this the factors stipulated to by Hammond in his guilty plea agreement such as the loss amount; the number of victims; and the sophisticated means and other specific characteristics of his offense. *See* United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") §§ 2B1.1(b)(1) and (2). The combination of these characteristics, along with his lengthy criminal history and acceptance of responsibility at his plea, results in a Guidelines range of 151 to 188 months' imprisonment. However, the applicable and stipulated Guidelines sentence is 120 months, the statutory maximum for the offense of conviction.

II. Discussion

A. The Nature and Circumstances of the Offense

The nature and circumstances of Hammond's offense support the substantial period of incarceration that is called for by the Guidelines. As set forth in the Complaint, the PSR, and the Background Section, Hammond played a central role in an extensive, deliberate, and destructive hacking campaign that caused widespread and serious harm.

The victims of Hammond's hacking included local police officers and their families, federal agencies, private companies, and thousands of private individuals. Hammond caused

substantial financial harm and emotional distress, violated privacy, and endangered public safety. As a result of his hacking activities, for example, the names, physical addresses, credit card data, and email addresses of thousands of clients of Stratfor were released and disseminated worldwide (PSR ¶ 23), resulting in approximately \$700,000 of unauthorized charges on those accounts (PSR ¶ 28), and cost more than \$1 million to Stratfor to repair. Brooks-Jeffrey Marketing, another of Hammond's victims, which maintains and services various law enforcement websites, suffered over \$280,000 in financial loss. (*See* Letter of BJM of April 17, 2013.) Vanguard calculated over \$70,000 in financial loss, and the Arizona Fraternal Order of Police, over \$20,000. (*See* Letter of [REDACTED] dated September 26, 2013 ("[REDACTED] Letter"); Letter of [REDACTED] dated September 25, 2013 ("[REDACTED] Letter").)

Moreover, much of the damage Hammond caused cannot even be quantified. A retired police officer and his wife, whose unlisted home phone number was released as a result of the AZDPS hack, received hundreds of harassing phone calls for weeks after – including physical threats. (*See* Letter of [REDACTED] dated August 12, 2013.) Indeed, the AZDPS – Arizona's statewide law enforcement agency – had to shut down its external email server, as well as its sex offender website and its fingerprint identification system, in order to address the damage from Hammond's hack. Arizona's Amber Alert System – which broadcasts "urgent bulletin[s] in the most serious child-abduction cases"¹⁴ – and that state's ability to track its

¹⁴ *See* Website of U.S. Department of Justice, AMBER Alert, America's Missing: Broadcast Emergency Response, <http://www.amberalert.gov/>.

aircraft and helicopters were also impacted by Hammond's cyber attack. (See Letter of ██████████ ██████████, Director, AZDPS, dated August 23, 2013.)

As a result of Hammond's related hack of the Arizona Fraternal Order of Police, the personal information, including the home addresses, of hundreds of active and retired law enforcement officers was disseminated online, and his hack of Vanguard released, among other things, the entire personal financial information of one of Vanguard's officers, all of which raised significant concerns about safety, privacy violations, and financial fraud for hundreds of individuals. (See ██████████ Letter; ██████████ Letter.)

Hammond played a leading role in all of these hacks, as well as other similar hacks described in the Background Section above, due mainly to his hacking experience and ability, as well as his relentlessness in identifying and attacking targets, particularly those tied to law enforcement. By his own account, his extensive involvement in computer hacking dates back at least a decade (Def. Mem. at 17), and his criminal hacking to at least 2005 (PSR ¶ 61). Indeed, it was Hammond himself who brought the AZDPS hack to LulzSec, his first foray with that hacking organization, bragging to the CW, "this time we have some high profile shit," uploading "a sample pdf" containing what appeared to be the name, phone number, and an e-mail address of an Arizona detective as evidence of what he had stolen, and then boasting later, "anyway, there's a LOT more where that came from."¹⁵ He then spent a few days going through the stolen material on his own, periodically sharing additional samples with his co-conspirators and the CW

¹⁵ (Bates # 78130-31.)

until he was ready to share the entire set of data, and he also contributed to drafting the press releases and strategized about the publicity campaign and release itself.¹⁶

Although Hammond does not appear to have initiated the Stratfor hack, he played a central role in that attack as well, in bringing it to fruition. In his submission, Hammond makes much of the CW's role in introducing Hammond to the hacker "hyrriiya" after the CW learned that hyrriiya claimed to have hacked into Stratfor. (Def. Mem. at 20-21.) Hammond elides over his own key role – which was to take over the hack from hyrriiya and carry it through to its successful completion. Indeed, about 20 minutes after the CW introduced them, Hammond informed the CW, "[i]t looks like he [hyrriiya] needs help breaking into their [Stratfor's] servers."¹⁷ And Hammond moved quickly to do what hyrriiya could not – completely penetrate and take over Stratfor's computer network. Hammond's criminal expertise and focus were instrumental to the success of the Stratfor hack.

Hammond played a similar central role in numerous other hacks, including those to which he pled, as well as a number of others, as described in greater detail in the Background Section. Notably, he worked on many of these on his own, as the evidence on his hard drive demonstrates – obtaining access to victim computer networks through vulnerabilities that he identified and that he knew how to exploit, and then stealing data, storing it on his hard drive, and going through it in detail before sharing it with others for release.

¹⁶ (Bates # 78128-78244.)

¹⁷ (Bates # 67014.)

Hammond's attempts to deflect blame or obfuscate his criminal activity are without merit. Among other things, Hammond claims in his sentencing submission that the CW actually participated in the Stratfor hack – rather than gathering information about it for law enforcement – by “providing servers for the storage of information and creating chatrooms to facilitate discussions.” (Def. Mem. at 21 and note 17.) This claim mischaracterizes the CW's role. As explained in the Complaint, the CW, at the direction of the FBI, provided to Hammond and his co-conspirators a server, which Hammond and his co-conspirators used to store the data they stole from Stratfor.¹⁸ (See Compl. ¶ 18j.) As a result of the FBI's control of this server, the FBI was able to mitigate the harm by, for example, notifying credit card companies about the compromised cards. The FBI's control of access to this server also would, and did, provide substantial evidence as to Hammond's identity and role in the attack. Similarly, the CW created chat rooms for Hammond and his co-conspirators at the direction of the FBI, which monitored the chats, gaining valuable intelligence about the hack which it used to notify Stratfor and credit card companies as the hack developed, as well as powerful evidence of Hammond's criminal activity.¹⁹

¹⁸ Indeed, as Hammond is aware, an encryption key that the CW passed to Hammond so Hammond could access this server was found on Hammond's hard drive, conclusively demonstrating that Hammond had accessed this server himself.

¹⁹ In an addendum to his sentencing submission, Hammond discusses additional hacks and conduct that he claims “provide the contextual framework for the Court's overall consideration of [his] intentions and motivation.” (Def. Exh. H at 1.) Specifically, Hammond alleges that the Government was “using [Hammond] to collect information regarding the vulnerabilities of foreign government websites and in some cases, disabling them.” (*Id.* at 2.) Hammond apparently reaches this dramatic conclusion based in part on a partially-redacted online posting by an anonymous individual who claimed to have hacked a foreign government at the behest of

B. History and Characteristics of the Defendant

Hammond's history and characteristics – in particular his unrepentant recidivism – also support a sentence of 120 months. Moreover, Hammond's claim now that his sole intent in engaging in the instant offense conduct was to serve the public good is false. As set forth below, the evidence shows that he was in fact engaged in a campaign of online sabotage, which damaged numerous websites and resulted in the unauthorized disclosure of the personal and financial information of thousands of individuals. Having previously received leniency in connection with his prior federal sentence for computer hacking, he is entitled to none in this case.

The defendant has an almost unbroken record of criminal offenses that demonstrate a total lack of respect for the law. As noted in the PSR, this prior criminal history includes, among others, a plea of guilty to criminal damage to property in 2003 (PSR ¶ 59), and convictions for battery in 2004 (PSR ¶ 60), disorderly conduct in 2006 (PSR ¶¶ 64-65), and mob action in 2009 (PSR ¶¶ 65-66), as well as multiple violations of supervised release, parole and probation (PSR ¶¶ 62, 64, 66, 68) and other arrests for disorderly conduct, contempt of court, and criminal trespass, among others (PSR ¶¶ 70, 72, 74, 75, 76, 77). Even more significantly, that prior criminal history also includes a federal conviction, in 2006, for the same offense – and

the CW. These claims are baseless. While the CW and Hammond did discuss vulnerabilities of foreign websites (among others), in fact, the FBI notified foreign governments about this activity and the vulnerabilities in their websites after Hammond was arrested and the CW's role could be revealed without harming the investigation so they could take appropriate remedial action. In any event, even if Hammond's allegations were true, which they are not, they do not bear on any issues relevant to sentencing.

essentially the same conduct – for which he is being sentenced here: the defendant hacked the website of an organization he disagreed with politically and obtained information such as the credit card numbers, home addresses and other identifying information of its members and customers. (PSR ¶ 61.) As here, he intended to make unauthorized charges using those stolen credit cards.²⁰ Hammond began engaging in his most recent hacking spree while serving a term of probation. (PSR ¶ 68.) Given that record, the Probation Office correctly notes in the PSR Hammond’s “propensity to continue to commit crime,” concluding that “[t]here is no information in his record that would suggest that he will not continue to recidivate.” (PSR, page 29 (“The defendant’s criminal record shows his disdain for the law as he has been cited for several violations while serving terms of supervision, along with two notable sanctions while housed at the Bureau of Prisons.”).)²¹

Hammond argues that he is entitled to leniency because he was motivated by altruism. (Def. Mem. at 28.) That claim is false. Hammond’s claim now that he was actually only engaged in a campaign of “civil disobedience” to expose government and corporate malfeasance is overwhelmingly contradicted by his own statements at the time of these hacks. Those statements to his confederates, long before he was arrested and when he did not expect to be caught, more likely reflect his true nature and intent rather than his post-hoc rationalizations now that he is actually being called to account for his actions.

²⁰ See Transcript of Sentencing, Dec. 7, 2006, Exhibit A (Bates # 000180 – 000222), at 15-17 (“Sentencing Tr.”).

²¹ Hammond violated Bureau of Prison rules by testing positive for marijuana and disobeying an order, resulting in sanctions including disciplinary segregation and loss of commissary, phone, and visiting privileges. (PSR ¶¶ 8-9.)

And what those statements generally demonstrate is that Hammond repeatedly expressed his goals to wreak havoc, damage law enforcement and anyone linked to it, and steal and disseminate financial information such as credit cards. Hammond bragged to his co-conspirators that he had “a three punch knockout plan” with regard to the stolen AZDPS data, and described one set of those materials as follows: “the last one was focused more on confidential documents/this one focuses more on personal email accounts, girlfriend pics, dirt and scandals.”²² In discussing the Stratfor hack, Hammond had extensive discussions about exploiting the stolen credit card information, including what to purchase with them,²³ and reveling in the chaos that he imagined would ensue. Hammond’s destructive goals are evident not only in his discussions about AZDPS and Stratfor but also many others. For example, Hammond bragged to the CW about the information he had stolen from Special Forces Gear:

[Hammond] the password list is fucking huge, and includes many .mil and .govs
 . . .

²² (Bates #078241-42.) A bit later, in the same chat, referring to one specific AZDPS employee, Hammond proposed, “if we drop AZ stuff on wednesday, we might want to pull some other prank, like change the AZDPS facebook group, his online dating profile or something silly.”

²³ For example, in a chat on December 19, 2011, Hammond said to his co-conspirators:

[Hammond] I was thinking we order some servers with them stolen CCs
 [Hammond] lots of servers with big hard drives
 [Hammond] and make four or five mirror .onions with them . . .
 . . .
 <~el che> getting servers with CCs
 [Hammond] it may be till the end of the mnth before the cc owner recognizes
 the bad charges

(Bates # 63171.)

[Hammond] furthemrrore
[Hammond] there are fuckloads of CCs
[Hammond] with expiration dates and addresses, but no CVV2s²⁴
[Hammond] if we can utilize this, we should, otherwise, we could just dump
itand watch the mayhem unfold.²⁵

Similarly, about the BPPA hack, he told the CW: “*gotta target the officers individually . . . i’ll put more work in later to see if we can destroy the site/we can do some cheesy defacement now by using their admin panel but it’s limited/its’ the only site on the server. . . .*”²⁶ Hammond expressed the same attitude about the hack into Combined Systems:

[Hammond] back on that combinedsystems box
[Hammond] there may be some good shit here
[Hammond] I dumped the db [database] again and saw more customers
[Hammond] some good, good customers
. . . .
[Hammond] but here is the paydirt friend . . .

This last boast is followed by Hammond’s “paydirt”: pages of what appear to be names, email addresses, physical addresses, and credit card numbers of numerous individuals, including police officers.²⁷

²⁴ “CVV2s” refers to “card verification value,” generally a three-digit code that typically appears on the reverse side of credit cards, as an anti-fraud measure often used for online transactions to verify that the credit card user is in possession of a valid credit card at the time of the transaction.

²⁵ (Bates # 67346.)

²⁶ (Bates # 67350 (emphasis added).)

²⁷ (Bates # 67584-67589.)

Hammond's own statements, while he was plotting and committing these attacks, demonstrate that his goals at the time were essentially to cause "mass mayhem" by destroying websites of entities he disliked, particularly related to law enforcement, and revealing stolen private information such as physical addresses, personal emails, and credit card data belonging to swaths of people remotely associated with those entities. Against this evidence, Hammond's claim now that his various law enforcement targets "were significant to [him] as a way of protesting police brutality, overly aggressive and militaristic anti-immigration laws and practices, and the governments' use of drones, tear gas and other weapons abroad" (Def. Mem. at 21) is, at best, beside the point.

There is nothing about this case that supports his argument for leniency now. It is notable that he has already been the beneficiary of leniency for his prior conviction, and the sentencing proceeding in that case is instructive. Hammond and his counsel argued for leniency then based on his youth and immaturity (he was 19 at the time), the absence of any malicious motive, and the fact that he did not actually make unauthorized charges on the stolen cards.²⁸

²⁸ See, e.g., Sentencing Tr. at 13 ((Hammond's counsel) ("In this case, he made a mistake. This one time, he took financial information that he shouldn't have had and did possess it. On the balance of that . . . he had that in his possession for a substantial period of time and did not benefit himself financially in any way. He did not steal from anyone.")); Sentencing Tr. at 17 ((Hammond's counsel) ("Mr. Hammond is in the possession of a very powerful, powerful power And I think that because of his age, because of the fact that, you know, he didn't show the responsibility that he needed to show utilizing that skill It's like bazookas in the hands of a child."); Sentencing Tr. at 19 ((Hammond) ("Although I clearly broke the law, my motivations were not to steal or to bring harm to anybody, physically or financially. . . . I was motivated out of altruism, not out of self-interest, not out of personal financial goals.")).

And the Court did substantially depart from the Guidelines, imposing a sentence of 24 months.²⁹

The sentencing judge explained his sentence to Hammond:

I believe you when you say that you have learned. I think, also, that after you're done serving your sentence, I would be willing to believe you if you told me that you understood precisely how damaging the democratic discourse of what you did is. I don't know that you fully understand that now. I concede that you fully understand what you did was wrong.

I believe that a 41-month sentence is too long in this particular case. It is, from my perspective, out of line with other sentences for computer hacking offenses, particularly those done out of unguided malice, a desire to wreak havoc, which motivates many hacking offenses, and those done for profit, and I suppose you could add to that those done to perpetrate particular harm against the named person. Yours, in many respects, is on the low end of the scale, but it's not at the bottom of the scale, because the prosecutor was right, that the damage you did, more precisely the threat of what you did, is damaging the democratic discourse, your side's as well as the other.³⁰

There are of course notable differences between his prior federal conviction and this offense: that case involved one website and actual loss of \$1,658, and the defendant did not in the end follow through with his plan to use the stolen credit cards.³¹ Unfortunately, though, Hammond did not learn, or at least not apparently anything positive, from the leniency shown to him then. In June 2011, barely a month after his term of supervised release ended (PSR ¶ 63), Hammond had already begun the conduct to which he pled guilty here: he approached the CW with his hack into the AZDPS, thus embarking on a hacking spree that dwarfed his 2006 offense

²⁹ The applicable guidelines range was 41 to 51 months. (Sentencing Tr. at 36.)

³⁰ Sentencing Tr. at 36-37.

³¹ Sentencing Tr. at 3-4, 24.

in scope, in volume, in the number of victims, in the losses caused, and in the damage done – not to mention that, this time, hundreds of stolen credit cards were in fact disseminated and used.

Hammond was given a substantial sentencing break when he committed his first federal offense. At the time, the judge explained his decision to be lenient by noting that Hammond’s crime was distinguishable from those hacking offenses which warranted substantial Guidelines punishment, pointing in particular to “those done out of unguided malice, a desire to wreak havoc, which motivates many hacking offenses.”³² Rather than heed the Court’s message, or even apparently reflect much on its leniency, Hammond then proceeded to undertake the same conduct the Court had cautioned against – but on a much greater scale – launching an online campaign of cyber attacks characterized by “unguided malice [and] a desire to wreak havoc.” Hammond’s history and characteristics fully support a sentence of 120 months.³³

C. The Need to Promote Respect for the Law, to Ensure Just Punishment, and for Deterrence in this Case

There is a critical need in this case to promote respect for the law and ensure just punishment. Hammond’s plea for a sentence of time served, that is, four months less than the 24-month sentence he received for his prior conviction (Def. Mem. at 34), should be rejected.

³² Sentencing Tr. at 36.

³³ As Hammond correctly notes in his sentencing submission, the Government is unaware of any evidence that he personally used the stolen credit cards or that he was motivated by personal financial gain. (Def. Mem. at 21.) Similarly, the Government has no reason to doubt that Hammond has been helpful and charitable to others, as many of his supporters attest, or that he also was motivated to contribute to the public good. In the Government’s view, these positive characteristics are significantly outweighed by the widespread harm he caused to so many, financially and otherwise.

After the leniency he received previously, he immediately re-engaged and expanded upon his prior offense – resulting in exponentially greater damage to thousands more victims.

Hammond’s assertion that he is “not without regret” that “private information of innocent parties was released to the public, and [for] any consequences suffered as a result of that breach of privacy” (Def. Mem. at 28) rings hollow, especially against his repeated contemporaneous expressions of the intent to cause precisely that harm on a mass scale. More leniency now would hardly serve as just punishment for a repeat offender nor would it serve as deterrence either to Hammond or to others who may be inclined to undertake similar activities. Hammond was already given a second chance to demonstrate that he could lead a law-abiding life. Instead, having been given leniency, he chose to dramatically escalate his prior offense in scope and consequences. As a result, he caused financial harm and emotional distress, violated privacy, and jeopardized public safety, to various entities and numerous individuals he had never met – in other words, he wreaked havoc, just as he hoped to. His conduct now deserves the strongest possible condemnation.

The factors that the Court is to take into account indicate that a sentence of 120 months is appropriate and warranted, principally due to the seriousness of Hammond’s offense, and the substantial harm he caused; his history and characteristics, in particular his recidivism; and the need for deterrence and just punishment.

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

3	UNITED STATES OF AMERICA,)	
4	Government,)	No. 06 CR 380
5	Vs.)	Chicago, Illinois
6	JEREMY ALEXANDER HAMMOND,)	December 7, 2006
7	Defendant.)	11:19 o'clock a.m.

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE JAMES B. ZAGEL
SENTENCING

For the Government:

THE HONORABLE PATRICK J. FITZGERALD,
UNITED STATES ATTORNEY
BY: Brandon D. Fox
Assistant United States Attorney
219 South Dearborn Street
Suite 500
Chicago, Illinois 60604

For the Defendant:

LAW OFFICES OF MATTHEW JOHN MCQUAID
BY: Matthew John McQuaid
53 West Jackson
Suite 1420
Chicago, IL 60604
(312) 726-9015

Court Reporter:

Blanca I. Lara, CSR, RPR
219 South Dearborn Street
Room 2504
Chicago, Illinois 60604
(312) 435-5895

1 THE CLERK: 2006 CR 380, United States versus
2 Hammond.

3 MR. FOX: Good afternoon, Your Honor.
4 Brandon Fox on behalf of the United States.

: 34 PM

5 MR. MCQUAID: Good afternoon, Your Honor.
6 Matthew McQuaid on behalf of Jeremy Hammond.

7 THE COURT: I see Mr. Hammond is here, as
8 well.

: 34 PM

9 PROBATION OFFICER ALPER: Good afternoon,
10 Judge.

11 Michael Alper on behalf of Probation.

12 PRETRIAL SERVICES OFFICER PAWLOWSKI: Good
13 afternoon, Your Honor.

: 34 PM

14 Amanda Pawlowski on behalf of Pretrial
15 Services.

16 THE COURT: Have both you and your client
17 seen the presentence report?

18 MR. MCQUAID: Yes, Your Honor.

19 THE COURT: And the supplemental report?

: 34 PM

20 MR. MCQUAID: Of the victim impact, Your
21 Honor?

22 THE COURT: Yes.

23 MR. MCQUAID: Yes, I have.

: 34 PM

24 THE COURT: And you have seen it, too,
25 Mr. Hammond?

1 MR. MCQUAID: We have not seen the victim
2 impact, Your Honor. I was shown that this
3 morning -- or this afternoon by Mr. Alper.

4 THE COURT: why don't you let him take a
5 quick look at this.

6 MR. FOX: I have a copy right here, Your
7 Honor.

8 THE COURT: Okay.
9 (Brief pause).

10 THE COURT: I have, in addition to that --
11 oh, do you and your client have any objections or
12 comments on this report other than your sentencing
13 memorandum?

14 MR. MCQUAID: No, Your Honor.

15 THE COURT: And then he can look at this one.
16 (Brief pause.)

17 MR. FOX: Your Honor, one thing with this
18 financial impact statement that we did receive, it's
19 my understanding from speaking with Mr. McQuaid that
20 there's no objection to providing [REDACTED] with the
21 restitution that he requests.

22 THE COURT: Did he tell this on his report --
23 oh, I see. He did tell it.

24 MR. MCQUAID: I believe \$1500, Your Honor,
25 and based on our plea of guilty --

:34PM

:34PM

:35PM

:35PM

:36PM

1 THE COURT: It's 1658.

2 MR. MCQUAID: 1658. He is accepting that.

3 THE COURT: All right.

4 And I have, in addition to the sentencing
5 memorandum, a long well-written letter from the
6 defendant's father.

7 MR. MCQUAID: Yes, sir.

8 THE COURT: Anything else that I should have?

9 MR. MCQUAID: No, sir, not on behalf of the
10 defendant.

11 THE COURT: Then you can begin.

12 MR. MCQUAID: Thank you, Your Honor.

13 would it be appropriate at this time,
14 Mr. Hammond, his father, would like to address Your
15 Honor or he would stand on the letter. I believe it
16 has been read.

17 THE COURT: Mr. Hammond, you can do this in a
18 short period of time?

19 MR. HAMMOND: I can do this in a very shortly
20 period of time.

21 THE COURT: Come on up, Mr. Hammond.

22 (Brief pause.)

23 MR. HAMMOND: Your Honor, you have read my
24 letter. Okay, I don't want to take too much past
25 that. I just want to emphasize, at one particular

:36PM

:36PM

:36PM

:36PM

:37PM

1 point the idea of a decision to commit a crime,
2 which I dealt with here. Jeremy had the possession
3 of those files for a long time and he decided not to
4 go ahead with the project and to leave the files,
5 essentially put the cash back.

6 His record with his work with other people,
7 and as far as I've known him, has been nothing but
8 for helping people, nothing but helping people and
9 working out with people.

10 On the Internet, he plugs people's holes.
11 Every person that does Internet security goes
12 through what Jeremy is going through right now, and
13 some day he will be quite an Internet security
14 professional.

15 I guess the bottom line is, judgment of
16 character. Will he do something like this again,
17 will he be a threat to society if he's allowed out
18 again. And I don't think anybody here is making
19 that case, and correct me if I'm wrong. And if
20 somebody is making the case that Jeremy is of poor
21 character, I would say that is certainly wrong.
22 Jeremy's instincts are good, his basic inner moral
23 core is good, and his sense of good and bad is good.
24 What's not good is, he was 19 years old and his
25 judgment was not good one time.

1 Early mistake and Jeremy realizes it, and we
2 realize the seriousness of such a charge. Internet
3 theft, if I had my credit cards on-line I would be
4 very happy that Mr. Fox and Mr. Brie from the FBI
5 was looking for the people that did that.

6 But Jeremy responded not for larceny, not for
7 politics, but Jeremy responded as revenge and waited
8 a long time before retaliating for people doing the
9 same type of thing to his site. I fully understand
10 it does not explain or excuse what he did, he went
11 over the line, but he did not search out a website
12 to pursue this scheme. He responded, he found the
13 credit cards, and later on he brain-stormed
14 different types of ideas and eventually the idea he
15 came up with was that he wasn't going to do anything
16 with them at all.

17 I guess everything else I need to say is in
18 the letter. I add one last thing, I am very, very
19 proud of my son and where he is in his life. I'm
20 not proud of this, but he's a good man, he's a good
21 person, and he's an honest person, and he's not
22 violent. And whatever your judgment is for him
23 today, I will still be proud of my son. He will be
24 a leader in everything he does the rest of his life.
25 I guess everything else I have to say is in the

1 letter.

2 Thank you very much, Mr. Zagel.

3 THE COURT: Go ahead.

4 MR. MCQUAID: Your Honor, when Jeremy Hammond
5 committed this offense, he was 19 years old, and he
6 stands before you as a 21 year old young man and --

7 THE COURT: Actually, I think I made a
8 mistake. I think we'll start with the prosecutor
9 and then go to you.

10 MR. MCQUAID: That's fine, Judge.

11 MR. FOX: That's fine, Your Honor. I can do
12 it either way. So that's fine.

13 THE COURT: Go ahead.

14 MR. FOX: I want to focus on a couple of
15 things on 3553(a), Your Honor. The first one is,
16 promote respect for the law, that's clearly
17 something that Your Honor has to consider in
18 sentencing the defendant.

19 This was not the defendant's first action on
20 the Internet that was unlawful. He also had the
21 D.A.R.E.com defacing where he went on to websites
22 to -- that was an anti-drug website, and he went on
23 that website, hacked into it, and put on there
24 pro-drug messages. And, you know, D.A.R.E. is about
25 children staying off drugs. And so by doing that,

1 he did hack into something that I think is an
2 important value to society. And, obviously, we
3 don't want our children on drugs, and if a child was
4 to go on the D.A.R.E. website and see a pro-drug
5 message, that's not something that's positive for
6 society.

7 He's also hacked into other servers,
8 including his former employer computer server at
9 NOC Specialist. And when he was at UIC, he was
10 kicked out of UIC for a hack. So when we're talking
11 about promoting respect for the law, Mr. Hammond has
12 not shown any respect for the law and he needs a
13 stiff sentence in other to be shown that he needs to
14 have respect for the law.

15 The other thing that Mr. Hammond needs to
16 have respect for, Your Honor, is other people's
17 opinions, because Mr. Hammond has shown in those
18 hacks, and in this hack in this case, that he
19 doesn't respect other people's opinions. We are a
20 society that is filled with people needing to have
21 respect for other people's opinions and their
22 speech; if we don't, our society breaks down.

23 If you look at some of the countries that are
24 unstable right now, these are countries where they
25 have religious battles, where people do not respect

1 each other's religious points of view or they have
2 political battles that are bloody instead of being
3 peaceful like we have in this country, and I think
4 that does come down to having respect for other
5 people's viewpoints.

6 And Mr. Hammond has strong political
7 viewpoints, and he should be commended for having,
8 for caring, for having strong political viewpoints,
9 but what he has to understand is that other people
10 can have those same strong viewpoints on the other
11 side and still have an important message. And this
12 is not a speech in saying that Mr. Hammond's
13 viewpoint is wrong or that [REDACTED] viewpoint is
14 wrong, because that's not my job here today.

15 I think the other thing that's important to
16 look at is deterrence. And Mr. Hammond is viewed as
17 a leader in the hacking community, and this is a
18 community that is sometimes on the outside of the
19 law and it needs to be reigned in. It needs to be
20 shown that hacking is not okay. It is not okay to
21 take someone else's property, to go on to somebody
22 else's property and take advantage of it. And I
23 think that a strong sense of this case would be a
24 deterrence for other people who are considering
25 hacking. And also for Mr. Hammond, it would be a

1 deterrence for him in the future that would make him
2 think twice before hacking again.

3 That's why I think, Your Honor, that it is
4 important to have a stiff sentence in this case.
: 43 PM 5 The guideline range, as you know, is above the
6 statutory maximum in this case. We are asking for a
7 sentence that is consistent with the statutory
8 maximum.

9 MR. MCQUAID: Your Honor, at the age of 19
: 43 PM 10 Mr. Hammond committed this crime. He is now
11 21 years old and he stands before you prepared to go
12 to jail for what he did.

13 And when he was 19 years old, Your Honor, he
14 was in possession of two skills. Two skills that he
: 43 PM 15 was highly qualified at, two skills that are not
16 common to most of the people that live in this
17 country: An amazing skill at computers. He can
18 walk into any computer and look around and see
19 everything that's been created, everything that can
: 43 PM 20 be done, everything that could be done at any point
21 in time at the beginning of the creation of the
22 program or the site and how far it could go. That's
23 the skill that most people don't have, very few
24 people do have. He had it, and he had it at a young
: 44 PM 25 age, a very young age, an emotionally young age.

1 And, I would say, at 19, he has not lived near as
2 much life as he needs to live to understand what
3 kind of power that is.

4 He also has a mind, a very strong mind, and a
5 mind that he uses to think about politics and social
6 change and things that are very volatile issues.
7 And he has a strong mind to understand what those
8 concepts are, what those policies are, how he agrees
9 or disagrees with them. And, again, Your Honor, in
10 the hands of a 19 year old, or in the mind of a
11 19-year old, Mr. Hammond is not emotionally equipped
12 to deal with all the emotions that came into him,
13 from these thoughts, from these viewpoints, from
14 these theories that he adopted.

15 He had two extremely strong, powerful talents
16 that he was just learning to understand how to
17 harness. To understand that when you have that much
18 power, when you walk down the line, the blue line
19 between good and evil, or choosing to do good and
20 choosing to do bad, you have to be responsible for
21 every decision that you make along the way. And
22 it's my opinion, Your Honor, that Mr. Hammond was
23 never emotionally mature enough at the point when
24 these two skills collided in this particular case,
25 or in his life at this time, for him to completely

1 control his anger or how he reacted to the feelings
2 that came across him when these things happened.

3 He developed these two skills, Your Honor,
4 the skill of the social and political thought in his
5 computer, and he put them into good use for most of
6 his life, for all of his life. He made good
7 decisions with those two things. He established a
8 food bank where he feeds poor people, part of the
9 social changes that he wants to affect on the world.
10 He and some colleagues take old bike parts, put the
11 bikes together, donate them to children that can't
12 afford them or people that can't afford them.

13 He put those same skills, those social chain
14 skills, along with his computer skills, and opened
15 up a computer lab using used computer parts in his
16 community, and then volunteers his own time to teach
17 those valuable computer skills to those of us who
18 aren't as skilled in the use of computers. He's
19 done things like that.

20 And he's organized, and he has leadership
21 abilities, and he's used that to try to affect
22 changes, positive changes in the world, and to do
23 good things with those skills. Tries to understand
24 what it takes to take the responsibility for the
25 gifts that one's been given.

1 In this particular case, Your Honor, the
2 prosecutor points out -- and when we use the word
3 "hacking," Your Honor, hacking is a skill. It has
4 good and bad people or people that choose to make
5 good and bad choices with that skill, but the
6 ability to get into a computer and use computers in
7 the way that Mr. Hammond is capable of is not
8 necessarily a bad thing. I'm not saying that
9 Mr. Fox is saying that, Your Honor, but I think it
10 needs to be clear, something that is new and
11 powerful in developing, and we all need to
12 understand what it is that hacking really is. In
13 this case, he made a mistake. This one time, he
14 took financial information that he shouldn't have
15 had and did possess it.

16 On the balance of that, Your Honor, he had
17 that in his possession for a substantial period of
18 time and did not benefit himself financially in any
19 way. He did not steal money from anyone. He did
20 not do that. And we can only speculate -- and I
21 know his father believes he wouldn't have, and I
22 believe he wouldn't have. And I know it's only
23 speculation to say what would have happened had he
24 not been caught, but in this case, he was not using
25 this for financial gain. And the evidence that was

1 prepared in this case indicates that there was never
2 a contention to line his own pockets or enrich
3 himself financially from the results of this
4 computer hack.

: 48 PM 5 Does he have instances of computer-type acts
6 that would necessarily be considered black hat?
7 Mr. Fox did bring up two and I have no dispute to
8 that, but not on the scale of where we're at, Your
9 Honor. Not the scale to say 5 years is appropriate
: 48 PM 10 for what he did in this case, and that's really
11 where we're at when it comes to sentencing, the
12 maximum amount of time should be given to him for
13 what he did in this case.

: 48 PM 14 THE COURT: Your theory is is that the
15 guideline cannot really be entirely correct or
16 appropriate in this case because it overstates the
17 loss.

18 MR. MCQUAID: I'm not trying to deprecate the
19 guidelines, but yes, I am saying that.

: 48 PM 20 THE COURT: He may very well have intended,
21 when he did it, to have a larger loss --

22 MR. MCQUAID: Than zero, yes. That's
23 possible.

: 48 PM 24 THE COURT: Right. But that he essentially
25 changed his mind.

1 MR. MCQUAID: Yes.

2 THE COURT: Okay.

3 Really, I don't initially view this -- and
4 I'm willing to accept the proposition that he's not
5 doing this for a gain in the traditional sense of
6 the word. He hacks into Protestwarrior.com, a site
7 which has views that, at the very minimum, you could
8 say he disagrees with and possibly which he finds
9 abhorrent. And he sets up a scheme by which the
10 various ProtestWarriors wind up having their credit
11 cards used for donations to charities and other
12 humanitarian organizations.

13 The pro-drug message on the D.A.R.E. website
14 may be a little harder to deal with, but we've dealt
15 with this kind of stuff before. I think his name
16 was Donald Segretti, worked for Richard Nixon, and
17 went to prison, and he printed false campaign
18 literature. My recollection, if I'm not mistaken
19 is, on somebody's letterhead, maybe Edmund Muskie's
20 letterhead, he sent out a letter accusing Senator
21 Jackson of Washington of having an illegitimate
22 child, which was complete fabrication. And there's
23 a certain number of people who found that amusing.
24 And, in a sense, it is amusing. And, in a sense,
25 it's amusing that you would take somebody's credit

1 card number and use it not to benefit yourself but
2 use it to support organizations probably which the
3 credit card owners would not particularly support.

4 But the government's response is is that this
5 is an area where cute does not mitigate the offense.
6 It's an area where people eager to promote whatever
7 cause they promote are entitled to the use of
8 various media. And even in Segretti's case, it's
9 campaign literature, which many people think to be
10 valuable. Personally, I regard it as a pain in the
11 neck when I get it, but many people don't.

12 Really, if you start interfering with this
13 stuff, if you start making people lose confidence in
14 their ability to support a particular cause of
15 whatever that cause is, you're altering some
16 fundamental preconditions for an effective democracy
17 while not actually changing the form of structure of
18 it. And that's really what has to be answered,
19 because I'm willing to concede this was not done for
20 personal profit. Personal profit had no role in it.

21 MR. MCQUAID: May I, Your Honor?

22 THE COURT: Yeah.

23 MR. MCQUAID: That is the hardest thing that,
24 as an advocate, I've had to deal with. These are
25 truly victims. These people had no ax to grind with

1 Mr. Hammond. They chose to support a particular
2 viewpoint, and, basically, they had their
3 information stolen. It's happened to me, not for
4 this reason, but I've had my information stolen
5 just because I trusted a website to be secure. They
6 didn't ask what was coming and he understands that.

7 And it is an offense punishable by prison,
8 Your Honor. And Mr. Hammond is not deprecating the
9 seriousness. He's not calling this, you know,
10 pizzas sent to a campaign office, things like that.
11 It's not a dirty trick. It's an imprisonable
12 offense. He's prepared to accept a prison sentence
13 in this case. I'm trying to ask Your Honor to take
14 a look at Mr. Hammond, this particular defendant,
15 what he did.

16 And I don't disagree with anything Your Honor
17 said, and I don't have any dispute what the
18 ramifications on our country is for people who do
19 these kind of things. It is a dangerous thing to
20 do. And Mr. Hammond is in the possession of a very
21 powerful, powerful power, is what I call it, because
22 it's something that most people can't do. And I
23 think that because of his age, because of the fact
24 that, you know, he didn't show the responsibility
25 that he needed to show utilizing that skill, these

1 skills. It's like bazookas in the hands of a child,
2 Your Honor, that's the kind of the way I look at it.

3 And I believe that prison -- I'm not asking
4 for probation. I'm not asking that he be sentenced
5 for 5 years based on who he is, on what he did do.
6 I think a sentencing range more towards the lower
7 end of prison is suffice to send that deterrent
8 effect to those who choose to use hacking or their
9 computer skills to do black-hat type of acts and
10 punish Mr. Hammond, accordingly, for what he did
11 based on who he is at this time in his life, and
12 give him the punishment and the deterrence that he
13 needs to go on after he is out of prison and he
14 still will be a young man, no matter what sentence
15 you give him, to be a responsible citizen.

16 THE COURT: Do you have any rebuttal to that?

17 MR. FOX: Your Honor, I think that you
18 expressed my viewpoint. So I don't have any
19 rebuttal for that. I agree with everything you say,
20 and Mr. McQuaid seems to agree with it, as well.

21 THE COURT: Mr. Hammond, do you want to say
22 something for yourself? Come to the center, it's
23 easier.

24 (Brief pause).

25 DEFENDANT HAMMOND: I prepared this, briefly.

1 Thank you.

2 First, I would like to take responsibility
3 for my actions. Although I clearly broke the law,
4 my motivations were not to steal or to bring harm to
5 anybody, physically or financially.

6 At the time, I was younger, and the whole
7 situation was taking place in a context of political
8 rivalry between a protest lawyer and other
9 republican counter-protest groups who were trying to
10 disrupt, you know, pro-peace marches and
11 demonstrations, both on the streets and on the
12 internet. There were small skirmishes taking place.

13 And although I had toyed with the idea of
14 making donations to humanitarian and charity groups,
15 which although it was very clearly against the law,
16 I was motivated out of altruism, not out of
17 self-interest, not out of personal financial goals.

18 All my life I have worked not out of
19 self-interest but to teach and share, you know,
20 skills and other organizing opportunities for
21 people. I want to help people. And since before
22 and after, and especially after, you know, I was
23 charged and indicted, I've been using the position
24 that I am with other people, you know, who look up
25 to me for having gone through, like, these computer

1 hacking charges and stuff, to share with them the
2 lessons that I have learned from these experiences.
3 And, in several cases, I've, you know, told people
4 who were as young and as reckless as I was at the
5 time not to get involved in this sort of, you know,
6 illegal direct action which would bring harm to
7 themselves and to others.

8 On the other hand, not just myself but the
9 people I work with, work as Internet security
10 experts and as hackers to help support, you know,
11 groups and organizations and institutions who try
12 to, you know, help people over here and around the
13 world.

14 Hackers are a necessary part of democracy, in
15 a sense, to help protect free speech on the Internet
16 and on the streets. And there's other community
17 programs that I've helped work with, such as Food
18 Not Bombs, which is like a community public serving
19 collaborative, because food is a right, not a
20 privilege.

21 I've helped build a community computer lab
22 out of spare parts, and helped teach people about
23 open source software, and otherwise provide, you
24 know, computers and printing to people who won't
25 otherwise have it; and other social justice-related

1 activism.

2 Essentially, all my years of being involved
3 in hacking and computer security, I have never
4 brought harm to, or stolen from, or done any
5 physical damage to a protest lawyer, or otherwise.
6 And although I broke the law, a prison sentence
7 would only unnecessarily bring harm to myself and
8 others.

9 And, essentially, no matter what happens
10 today, I'm going to use this opportunity that, you
11 know, it's not the end, you know, of my life here.
12 That I'm going to continue my work and research in
13 trying to help the community, and sharing skills,
14 and otherwise. So my goals are to help people.
15 That's all I really have to say.

16 THE COURT: I'm going to ask you a couple of
17 questions, but I want to tell you, you don't have to
18 answer this. You are not obliged to answer any of
19 my questions. And if you don't want to, you don't
20 have to.

21 Talk to me about D.A.R.E., the D.A.R.E. site
22 and why you did what you did.

23 DEFENDANT HAMMOND: well, at the time, it was
24 even before the protest lawyer incident, D.A.R.E.com
25 being in what many people feel--I know it's not the

1 position of the state--but as a tool to use to,
2 like, promote the war on drugs which many people
3 feel are putting many people in jail unnecessarily,
4 millions of people, for crimes when there are
5 greater crimes.

6 So, essentially, what happened was, a few
7 people put up a message on D.A.R.E.com's website.
8 It was up for a couple of hours, and it,
9 essentially, was like a criticism of the D.A.R.E.
10 program. There's no damage done to the server, no
11 files were deleted. It was back on line in, like, a
12 day or something like that.

13 THE COURT: Do you remember what the message
14 said?

15 DEFENDANT HAMMOND: I don't have it in front
16 of me right now. It did make a reference to such as
17 why is tobacco and alcohol, like, not only legal but
18 promoted by, you know, television and commercials,
19 and stuff like that, while at the same time millions
20 of people are put away for the use of marijuana
21 which does far less harm than alcohol, tobacco, and
22 if not less, then at least the same harm.

23 So, essentially, it was not necessarily a
24 pro-drug statement, but more like instead of someone
25 going to D.A.R.E.com and ordinarily seeing the same

1 facts and stuff that D.A.R.E. would normally put up,
2 that it would provide not an opposing viewpoint but
3 an alternative viewpoint.

4 THE COURT: Stop for a second.

5 :00PM Is that about right, from the government's
6 perspective?

7 MR. FOX: That is consistent. Mr. Hammond
8 also put out a message about his girlfriend at the
9 time, is my recollection. We don't have a printout
10 :00PM of that website, so we don't have anything to the
11 contrary.

12 THE COURT: If his description is
13 approximately true, is what I want to know.

14 MR. FOX: And if I could, Your Honor, if I
15 :01PM may respond to the one point that he's made. There
16 are plenty of websites that have the type of message
17 that Mr. Hammond was trying to create on that
18 D.A.R.E.com website, the fact is that he was trying
19 to stop D.A.R.E. speech from coming out.

20 :01PM THE COURT: No, I understand, but the
21 substance of the message matters.

22 MR. FOX: I can't dispute that at this point.

23 THE COURT: All right.

24 And why did you stop short with respect to
25 :01PM the charitable humanitarian donations?

1 DEFENDANT HAMMOND: well, I had been talking
2 to a few close colleagues and activists, at the time
3 I was already in a certain amount of trouble because
4 I was facing state charges and stuff, who thought
5 that this would probably bring increased repression
6 down not just on myself but on other people, as
7 well, if we were to carry through the plot, and it
8 would probably end up doing more damage to the left,
9 anyway, like if we had gone through with it. In
10 fact, at the time, I felt that it would be making
11 more of a statement if we actually had access to the
12 stuff and didn't go through with the plot than if we
13 actually would have had to.

14 THE COURT: Thank you.

15 There's one issue that I do want to address
16 with counsel and that is the guideline calculation.

17 The guideline calculation is, obviously, an
18 intended loss calculation, and I do have some
19 difficulty with applying it, and the reason I have
20 some difficulty with applying it is, the fairly
21 unique situation we face here.

22 Ordinarily, you apply intended loss where
23 somebody intends to cheat another person out of
24 2 million dollars and then they start down that road
25 and they get caught. And they may take nothing,

1 they may take a small amount, and we count 2 million
2 dollars against them because that was their intent.
3 And for people who don't have a particularly
4 intended loss, we count the loss that they actually
5 inflicted.

6 In this case, we have an intended loss that
7 might be quite large, but it wasn't carried out, and
8 the reason it wasn't carried out had nothing to do
9 with his getting caught, it had to do with the fact
10 that he changed his mind.

11 So at the time that he's actually
12 apprehended, what we have is a loss that I would
13 have some difficulty classifying as intended in the
14 sense that it was intended at one point -- in the
15 fairly technical and arbitrary way in which the
16 guidelines deal with intended loss, because people
17 rarely have a specific intent with a specific number
18 in mind, but, realistically, we deal with that
19 because we see where the scheme might have gone, we
20 see what the consequences would have been, even if
21 the calculation has not been made by the
22 perpetrator. And we probably have that in this case
23 where he hasn't made an actual calculation, but he
24 subverts his own intent later on, and the usefulness
25 of using the full intended loss in this case strikes

1 me as raising a question. So you can speak to that
2 one.

3 MR. FOX: In terms of the strict guideline
4 application, Your Honor, I think it's right that the
5 guideline calculation is the 2.5 million using the
6 \$500 a credit card. It's an issue I looked at
7 before we even charged this case and I did research
8 on it. I agree with Your Honor that it's a unique
9 case.

10 And, ultimately, what I came to was, if you
11 look at 2B1.1, its provision in the notes regarding
12 stolen or counterfeit credit cards, it doesn't
13 mention anything there about fraud, it just talks
14 about the value of the credit card. And what
15 Mr. Hammond took, they were credit cards, and if you
16 went with their intrinsic value of \$500 per credit
17 card, that's where you come to it, and that's where
18 I think the guidelines are talking about it.

19 There is no law that I found on this. So
20 Your Honor might be doing something here novel which
21 may or may not be appropriate considering a
22 guideline calculation versus just considering what
23 you're talking about under 3553(a). I think
24 probably under the guidelines, that the proper
25 allocation is \$500 per card, I think Your Honor can

1 consider his intent under 3553(a).

2 THE COURT: Mr. McQuaid, you want to speak to
3 that point?

4 MR. MCQUAID: Your Honor, when I looked at
5 the application note 3F1--and, again, I agree with
6 Mr. Fox--I mean, there's nothing about the
7 application of the guidelines, using the guidelines,
8 that I find inappropriate. However, when I look at
9 the application note 3F1 and I see that in any case
10 involving a counterfeit access device, in this case
11 being the possession of the credit card numbers, and
12 they apply a \$500 per access device, I did make an
13 interpretation that this is referring to actual loss
14 and intended loss. If someone did use the credit
15 card and did not charge up to \$500, I think what the
16 guideline is trying to say is that, at the very
17 least, the victim's card should be given the
18 appropriate monetary weight, that being 500, so the
19 defendant, in particular, having harmed the victim
20 in this way, even at a low amount, let's say 25 or
21 50 dollars, should be punished for the utilization
22 of the card.

23 It goes on further to note that there is
24 another situation where "if the unauthorized access
25 devices is a means of telecommunication access," and

1 I can't tell Your Honor if I have any idea of what
2 that means, but it does indicate that it's basically
3 information that is in mere possession of the
4 defendant and then classifies that mere possession
5 of that information, that counterfeit access device,
6 at the level of \$100.

7 So there seems to be a case where we might
8 have possession which could have maybe a lesser
9 monetary qualification than \$500. And I'm not
10 saying that that makes any sense, Your Honor, but
11 when I was reading it and trying to think about it,
12 trying to make an argument that, you know, would
13 fly, that did cross my mind, that it is a monetary
14 amount that would be applied to actual loss, as
15 well. That if it was not used up to 500, it would
16 be given \$500 worth of credit, and they do make a
17 distinction in mere possession of another type of
18 access device that mere possession is only \$100. So
19 I believe there is some -- there could be some
20 fluctuation in the loss amount even using the
21 guidelines, possibly.

22 MR. FOX: Your Honor, if I may respond to
23 that real quick. The probation officer, who is in
24 agreement with me on this, the telecommunications
25 instrument or account that they talk about is a

1 phone card, it's not a credit card, so that's the
2 distinction, because certainly phone cards have less
3 of a value than credit cards do.

4 THE COURT: In a sense, I believe the
5 guideline is correctly calculated if you read
6 literally, but I believe that I'm thinking of
7 departing on 5K2.0A3.

8 MR. FOX: 5K? What was it, Your Honor?

9 THE COURT: 5K2.0A3. A 3, the title explains
10 it all:

11 "... departure is based on circumstances present
12 to a agree not adequately taking into
13 consideration"

14 and the reason I believe that the
15 circumstances are not adequately taken into
16 consideration are two:

17 The first is, this is a case in which the
18 guideline calculation, appropriately made, at its
19 high end, exceeds the maximum sentence. Because it
20 exceeds the maximum sentence, I regard that as, at
21 least, evidence that the guideline calculation
22 significantly outstripped, outstripped to some
23 extent, the Congressional intent in passing the
24 statute with a maximum sentence. It's not
25 necessarily the case, but it's one thing that points

1 me in the direction of believing that 5K2.0A3 would
2 apply here.

3 More significantly, is the complete absence
4 of any specific addressing within the guidelines of
5 the issue present here where somebody forms an
6 intent to inflict a loss, and then before the loss
7 is inflicted, changes that attempt. It's not
8 addressed in the guidelines.

9 More importantly, even than that, is the fact
10 that there is really no case law on it, which says
11 to me that it is unique. It doesn't happen very
12 often. And it is precisely the kind of thing that
13 the Sentencing Commission could not be expected to
14 take into account and didn't take into account. So
15 I believe that a departure is called for.

16 And I intend to calculate the guideline, even
17 though the guideline is no longer binding on me,
18 because I think it is appropriate to do so. And
19 unless anybody has anything further to add, I will
20 tell you approximately what my calculation would be.

21 MR. FOX: Your Honor, let me just make sure
22 that I'm understanding. Because the Seventh Circuit
23 has said that departures are obsolete at this point
24 based on Booker, my understanding is that you're
25 looking at this grounds for departure in order to

1 adequately calculate the loss figure as kind of
2 guidance for the loss figure, is that what you're
3 saying?

4 THE COURT: Yes.

5 MR. FOX: Okay.

6 THE COURT: It's not a departure in the sense
7 that the Seventh Circuit has said is irrelevant.
8 It's a departure which justifies the recalculation
9 of the guideline, and that's assuming that the
10 Seventh Circuit's view that departures no longer
11 matter is valid, and there's other circuits that
12 disagree, but it's not that kind of departure that
13 we're talking about.

14 MR. FOX: Thank you, Your Honor.

15 THE COURT: Do you have anything to add?

16 MR. MCQUAID: No, Your Honor.

17 THE COURT: My view is this, the full loss
18 calculation -- let me get back to that one in the
19 book.

20 MR. FOX: In the new book, Your Honor, it's
21 on Page 75.

22 THE COURT: There is a temptation to reduce
23 it to close to zero, but we actually know there was
24 a loss, but it falls into that category. But I
25 don't think that would be right either because there

1 was certainly a period of time when there was a
2 substantial risk of a very large loss, and a risk
3 not only from the defendant but a risk that perhaps
4 he might have lost control of the data and someone
5 else might have taken advantage of it. And the risk
6 of loss to the victim, that he inflicted on the
7 victim for a period of time before he ultimately
8 decided not to do it, I think, is substantial.

9 what I think the more appropriate calculation
10 in all of this is entirely hypothetical because I'm
11 looking back at an event that we know happened and
12 there's no way for me to calculate what the
13 probability would have been that he would have
14 changed his mind when he did it. But I think given
15 his justification for doing what he did, given the
16 fact that he was more interested in countering
17 speech that he found wrong than he was in picking
18 the pockets of those uttering the speech, that the
19 appropriate adjustment level in this case would be
20 an adjustment -- and this, of course, is a guess,
21 but I believe the chance at initiation that he would
22 have actually carried this out is perhaps 30 percent
23 and I believe the correct guideline calculation
24 would then be 30 percent of 2 million.

25 MR. FOX: I think that's about 800,000, it's

1 a little more than 800,000, but that falls right
2 between more than 400, less than a million, which
3 would be a 14 level increase, Your Honor.

4 THE COURT: The calculation is what?

:19PM 5 MR. FOX: One-third of -- I'm doing one-third
6 of 24 million which -- or 2.4 million, which would
7 be 800,000. I'm guessing .3 of 2.5 can be around
8 the same figure, so I'm getting 800,000,
9 approximately, as a loss, which would fall between
:19PM 10 the 400,000 and 1 million as a loss figure under the
11 guidelines.

12 THE COURT: what is your base you're figuring
13 this on?

14 MR. FOX: I'm looking at, if I'm not
:19PM 15 mistaken, Your Honor, 2B1.1.

16 THE COURT: Right. But the loss level
17 calculated is?

18 MR. FOX: In looking at over \$400,000, it
19 says add 14.

:20PM 20 MR. MCQUAID: Less than a million.

21 THE COURT: Right. But the calculation, the
22 base is \$2,500,000.

23 MR. FOX: Right.

24 THE COURT: And 30 percent of \$2,500,000 is?

:20PM 25 MR. FOX: Close to 800,000.

1 THE COURT: Right.

2 MR. FOX: Yes.

3 THE COURT: which takes him to offense level
4 21 for guideline purposes, 21.2, which is 41 to
5 51 months.

:21PM

6 Anybody have anything further to say?

7 MR. FOX: Not from the government, Your
8 Honor.

9 MR. MCQUAID: No, sir.

:21PM

10 THE COURT: Mr. Hammond, you want to come to
11 the center. Right there. Stand in the middle.

12 (Brief pause)

13 THE COURT: This case presents--although I
14 suspect, Mr. Hammond, you have not spent a lot of
15 time studying the history of sentencing--the problem
16 we always have with gifted people, and you do have a
17 gift, is that the defense lawyer, and in this case
18 your father as well, will point to a gift as a great
19 mitigating factor, but that's not right.

:21PM

20 The prosecutors will sometimes point to it as
21 a great aggravating factor on the theory that
22 somebody with a gift has a special responsibility to
23 use it wisely and within the law. And I don't think
24 that's true either.

:22PM

25 A gift is very much like a firearm. It

:22PM

1 depends entirely on how it's used. So I don't give
2 you the credit or debit for the fact that you have a
3 gift. I do consider what your father said as true.
4 And I don't think your father actually uses these
5 words, but the core of his message is that you were
6 19 years old and you were an idiot when you did
7 this. And although I suspect there is some people
8 in this courtroom of whom I can see who are not that
9 far over 19 years of age, I can tell you that, from
10 the perspective of my age, all 19-year olds are
11 idiots. So I'm willing to accept that, as well.

12 And what young people have the most
13 difficulty dealing with is playing by rules. And
14 they have the single greatest difficulty playing by
15 rules when they see that some opponent of theirs or
16 believe that some opponent of theirs is not playing
17 by the rules. And one of the great lessons of
18 adulthood and one of the foundations of our society
19 is, that it's not a defense to an allegation of rule
20 violation that your opponent violated the rules, as
21 well. It's not a defense to a charge of cheating
22 that your opponent was cheating. Understandable,
23 but not a defense.

24 The other aspect of this case is is that,
25 like the firearm, the gift you possess has a lot of

1 power in it. Segretti, who I mentioned before, used
2 the printing press, something which also has a lot
3 of power. And he used the media and television and
4 a variety of other things, and if he had done the
5 same kind of thing today, he'd use the web. And he
6 went to prison, and you're going to go to prison,
7 the question is for how long.

8 The guideline says 41 to 51 months. And I
9 don't have to follow the guideline and I'm not going
10 to follow the guideline. I believe you when you say
11 that you have learned. I think, also, that after
12 you're done serving your sentence, I would be
13 willing to believe you if you told me that you
14 understood precisely how damaging the democratic
15 discourse of what you did is. I don't know that you
16 fully understand that now. I concede that you fully
17 understand what you did was wrong.

18 I believe a 41-month sentence is too long in
19 this particular case. It is, from my perspective,
20 out of line with other sentences for computer
21 hacking offenses, particularly those done out of
22 unguided malice, a desire to wreak havoc, which
23 motivates many hacking offenses, and those done for
24 profit, and I suppose you could add to that those
25 done to perpetrate particular harm against the named

1 person. Yours, in many respects, is on the low end
2 of the scale, but it's not at the bottom of the
3 scale, because the prosecutor was right, that the
4 damage you did, more precisely the threat of what
5 you did, is damaging the democratic discourse, your
6 side's as well as the other. And to deter others, I
7 think you have to go to prison.

8 The sentence of the Court is 24 months in the
9 custody of the Bureau of Prisons, to be followed by
10 a period of supervised release of 3 years. I'm
11 assessing a fine of \$3,600. I'm ordering
12 restitution to be paid to [REDACTED] in the amount
13 of \$1,658, and I'm also imposing a \$100 assessment.

14 The conditions of supervised release would be
15 that within 72 hours of release from the custody of
16 the Bureau of Prisons you have to report in prison
17 to the Probation Office in the district to which you
18 are released. You may not commit another federal,
19 state or local crime, you can't violate any criminal
20 law of any jurisdiction.

21 You have to abide by the standard conditions
22 that have been adopted by this court. You must
23 refrain from any unlawful use of a controlled
24 substance, you must submit to one drug test within
25 15 days of release, and as many random drug tests as

1 the Probation Office orders, except it can't exceed
2 104 tests per year.

3 If there is a restitution balance left over
4 at the end of your term, your monthly payment will
5 be 10 percent of your net monthly income. You shall
6 participate in a drug-after care treatment, which
7 may include testing at the direction of the
8 probation officer.

9 During the period of supervised release, you
10 should have no involvement with hackthiscite.org or
11 related electronic civil disobedience in websites
12 and organizations, and you shall have no involvement
13 or contact with the Chicago Anarchist Network or
14 related civil disobedience organizations. You may
15 not possess a firearm or destructive device.

16 It's not that you picked the wrong side or
17 the right side, Mr. Hammond, it's that you picked up
18 the wrong weapon to wield in support of the side you
19 picked.

20 Surrender date?

21 MR. FOX: Your Honor, both Pretrial Services
22 and Probation have expressed to me their belief is
23 that Mr. Hammond should report today, that he should
24 be taken into custody.

25 I can tell you from Pretrial Services

1 perspective, that Mr. Hammond has not reported for
2 three weeks, that he's also failed two drug tests,
3 and during the period that he has been on supervised
4 release Mr. Hammond has been arrested twice. So he
5 has not been in compliance with term of supervised
6 release.

7 THE COURT: The two arrests, were those the
8 ones that I dealt with earlier?

9 MR. FOX: You dealt with one and then there
10 was a separate one, my recollection is. And I can
11 also tell you that after you dealt with his arrest
12 when he was in court before, you know, since then,
13 he hasn't reported to Pretrial Services for the
14 three weeks. So even though after you admonished
15 him, he didn't comply with conditions.

16 PRETRIAL SERVICES OFFICER PAWLOWSKI: Your
17 Honor, one arrest occurred June 8th, he had been
18 arrested and has plead guilty and sentenced to
19 6 months. The second arrest was September 7th,
20 failed to report to the Cook County Probation
21 Officer and I believe he has now satisfied the term
22 of probation, but he failed to report to her and
23 that's why he was arrested in September.

24 MR. MCQUAID: I believe Mr. Hammond was aware
25 of his responsibilities, Your Honor. I believe his

1 last drug test was negative. I'm asking that he at
2 least stay out until after the holidays, Your Honor,
3 three weeks.

4 THE COURT: Surrender date is January 3rd.

5 You do have the right to appeal the sentence
6 which I've imposed upon you. And if you want to do
7 that, talk to Mr. McQuaid, he'll tell you how to go
8 about doing this.

9 There is one other thing I ought to tell you
10 too, because of what happened in the pretrial
11 administration of this. When you're on supervised
12 release, if you disobey the conditions of supervised
13 release, you're basically subject to the kind of
14 sentence that I didn't give you this time. And it's
15 not a mere condition. You, actually, have
16 surrendered a lot when you plead guilty, more than
17 maybe you think, because it's not just the 24 months
18 and whatever pain in the neck there is at dealing
19 with the probation officer. It's the fact that, for
20 example, you couldn't own a firearm, even if you
21 wanted to. You have to submit to some restrictions,
22 some of them may be, from your point of view,
23 arbitrary, some of them may even mean, from my point
24 of view, arbitrary, and you have no right to say no.
25 It's a real loss of rights and abilities. And it's

1 important that you understand that, because if you
2 tread over the line during the period of supervised
3 release, you could very easily end up in the Bureau
4 of Prisons. And there was a lot to be said for when
5 imposing a higher sentence in this case, but I
6 believe you have learned your lesson about limits,
7 and that's the only thing we're talking about.
8 We're not taking about your views, we're talking
9 about limits, but those limits are there and they
10 are tighter than they would be on an ordinary
11 citizen during the period of supervised release.
12 Don't miss the surrender date.

13 Anything further?

14 MR. FOX: Your Honor, if I may have a moment
15 with Mr. McQuaid?

16 THE COURT: Yes.

17 (Brief pause)

18 MR. MCQUAID: Mr. Hammond is requesting if
19 the Court can recommend an institution closest to
20 his family in Illinois.

21 THE COURT: Yeah, I'll make a recommendation
22 that the institution be as close as possible to
23 Chicago.

24 MR. FOX: And, Your Honor, I do want to
25 state, I don't think the BOP will have made its

1 designation by January 3rd, so I ask Your Honor to
2 order Mr. Hammond to report to probably the MCC.

3 THE COURT: Yeah, he will report, he'll have
4 to report to the MCC.

:34PM

5 MR. FOX: Or the marshal's office here.

6 THE COURT: Or the marshal's office, yes.
7 Anything further?

8 MR. MCQUAID: No, sir. Thank you.

9 THE COURT: Thank you.

:35PM

10

11 (Which concluded the proceedings had on this
12 date in the above entitled cause.)

13

14

15

16

17

* * * * *

18

19

20 I CERTIFY THAT THE FOREGOING IS A CORRECT TRANSCRIPT
21 FROM THE RECORD OF PROCEEDINGS IN THE ABOVE-ENTITLED
22 MATTER

23

24

25

/s/Blanca I. Lara

date

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Blanca I. Lara

Date