UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- x
:
UNITED STATES OF AMERICA
:
- v - 11 Cr. 666 (LAP)
:
HECTOR XAVIER MONSEGUR,
a/k/a "Sabu," :

Defendant. :
- x

GOVERNMENT'S NOTICE OF INTENT TO MOVE PURSUANT TO SECTION 5K1.1(A)(1)-(5) OF THE SENTENCING GUIDELINES AND PURSUANT TO TITLE 18, UNITED STATES CODE, SECTION 3553(e)

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

JAMES J. PASTORE, JR.
Assistant United States Attorney
- Of Counsel –

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v -	:	11 Cr. 666 (LAP)
HECTOR XAVIER MONSEGUR, a/k/a "Sabu,"	:	
Defendant.	:	

Preliminary Statement

The Government respectfully submits this memorandum in connection with the sentencing of defendant Hector Xavier Monsegur, a/k/a "Sabu" (the "defendant" or "Monsegur"), which is currently scheduled for May 27, 2014 at 11:00 a.m. In its Presentence Report ("PSR"), the United States Probation Office ("Probation") correctly calculates that the defendant's United States Sentencing Guidelines ("U.S.S.G." or "Guidelines") range is 259 to 317 months' imprisonment. Probation recommends a sentence of time served. As set forth in more detail below, Monsegur was an extremely valuable and productive cooperator. Assuming that the defendant continues to comply with the terms of his cooperation agreement, and commits no additional crimes before sentencing, the Government intends to move at sentencing, pursuant to Section 5K1.1 of the United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") and Section 3553(e) of Title 18, United States Code, that the Court sentence the defendant in light of the factors set forth in Section 5K1.1(a)(1)-(5) of the Guidelines, and without regard to the otherwise applicable mandatory minimum sentence in this case.

Statement of Facts

I. Monsegur's Involvement with Anonymous, LulzSec, and Major Cyber Intrusions

Throughout 2011, hackers affiliated with the "Anonymous" movement targeted hundreds of computer systems around the world, hacking, disabling and at times exfiltrating data from those systems. Victims included news media outlets, government agencies and contractors, and private entities. In approximately May 2011, Monsegur and five other members of Anonymous formed Lulz Security, an elite hacking collective or "crew" commonly referred to as "LulzSec."[1] Monsegur and the other core members of LulzSec typically worked as a team and had complementary, specialized skills that enabled them to gain unauthorized access to computer systems, damage and exploit those systems, and publicize their hacking activities. This core group, among whom only Monsegur was identified prior to the time Monsegur began cooperating in the investigation, included:

- Monsegur, a/k/a "Sabu," who served primarily as a "rooter," analyzing code for vulnerabilities which could then be exploited;
- "Kayla," who specialized, among other things, in "social engineering" – that is, manipulating others into divulging personal information such as login credentials;
- "T-Flow," who served as an organizer, analyzing information provided by members of the group in order to direct other members what to do next;
- "Topiary," who served from time to time as the public face of Anonymous and LulzSec, giving interviews to media outlets and writing public communications on LulzSec's behalf;

[1] "Lulz" is shorthand for a common abbreviation used in Internet communications – LOL – or "laughing out loud." As explained on LulzSec's website, LulzSec.com, the group's unofficial motto was "Laughing at your security since 2011."

- "AVUnit," who provided computer infrastructure for the group such as servers; and
- "Pwnsauce," who performed some of the same work as Monsegur and Kayla.

Monsegur and many of these core LulzSec members were also part of another Anonymous-affiliated group called Internet Feds which, like LulzSec, engaged in major criminal computer hacking activity.

Throughout 2011, Monsegur, through LulzSec and Internet Feds, engaged in several major hacks into and thefts from the computer servers of United States and foreign corporations and other entities including the following:

- HB Gary. Monsegur directly participated in the hack of the computer system of this internet security firm in response to the firm's claim, through one of its investigators, that it had identified the members of Anonymous. This hack involved the theft of emails and other company information.
- Fox Television. This hack resulted in the compromise of a database of contestants of a reality TV show called "X-Factor." Monsegur downloaded data from Fox that he was able to obtain through his co-conspirators' unauthorized access to Fox's computer systems.
- Tribune Company. A journalist provided his credentials to Internet Feds in the hopes he would be invited into private chats. Monsegur used the credentials to login to the Tribune's systems and confirmed that the credentials could be used to gain access to Tribune Company's entire system.

- PBS.org. Monsegur was a direct participant in this hack, which resulted in the compromise of PBS's servers and the defacement of its website. Monsegur helped identify a vulnerability and then installed multiple "back doors" on PBS's system – that is, he installed programs that allowed others to later access the computer system.[2]

- Sonypictures.com. Monsegur was a direct participant in this hack, in which the personal identification information of customers was stolen from Sony.

- Sony BMG sites in Belgium, Russia, and the Netherlands. Monsegur accessed and downloaded data from the Belgium and Netherlands sites, including the release dates of records. Monsegur passed information about a vulnerability for the Russian website to other members of LulzSec for exploitation.

- Nintendo. Monsegur participated in a hack into Nintendo's computer systems, pursuant to which files regarding the structure of Nintendo's computer systems were downloaded.

- Senate.gov. Monsegur had knowledge of, and conducted research for, this hack of the Senate's website.[3]

- Bethesda/Brink video game. Monsegur helped hack into Bethesda's system, and downloaded information including a database containing personal identification information.

- Infragard/Unveillance. Monsegur was a participant in a hack of an FBI affiliate in Atlanta, which resulted in the theft of confidential information.

---

[2] Following his arrest, Monsegur provided information that helped repair and remediate this hack.

[3] Monsegur provided the FBI with information about the vulnerability, which allowed it to be repaired or "patched."

In addition to Monsegur's direct participation in the criminal hacking activity set forth above, Monsegur had contemporaneous knowledge of other major criminal hacking activity by his co-conspirators, including hacks into the computer servers of the Irish political party Fine Gael; a U.S. online media outlet, [redacted] a foreign law firm, [redacted]; and the Sony Playstation Network.

In addition to the six "core" members identified above, several individuals were loosely affiliated with Monsegur and LulzSec, including, significantly, Donncha O'Cearrbhail, a/k/a "palladium," and Jeremy Hammond, a/k/a "Anarchaos." Hammond, the FBI's number one cybercriminal target at the time of his arrest in 2012, 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 in which he broke into these victims' computer systems, stole data, defaced websites, destroyed files and published online the sensitive personal and financial information of thousands of individuals – all with the object of creating, in Hammond's words, maximum "mayhem."

The hacks identified above constitute only a portion of the significant criminal computer intrusions committed by Internet Feds, LulzSec, and their members, including Monsegur. As the examples make clear, Monsegur and his co-conspirators indiscriminately targeted government agencies, private companies, and news media outlets. In many instances, the harms inflicted on these entities were significant, ranging from defacements of their websites to the exfiltration of personal identification information of customers or employees of the entities; the costs associated with repairing these attacks ran into the tens of millions of dollars. Monsegur was a key participant in these Anonymous hacking crews, providing his technical expertise to aid in many of the hacking operations.

II. The Complaint, Monsegur's Guilty Plea and Subsequent Remand, and the Guidelines Calculation

On or about June 7, 2011, the FBI approached Monsegur in his home and questioned him about his online activities. Monsegur admitted his criminal conduct and immediately agreed to cooperate with law enforcement. That night, Monsegur reviewed his computer files with FBI agents and provided actionable information to law enforcement. The next morning, Monsegur appeared in court on a criminal complaint charging him with credit card fraud and identity theft, and was released on bail, whereupon he immediately continued his cooperation with the Government, as described further below. On or about August 15, 2011, Monsegur appeared before Your Honor and entered a guilty plea pursuant to a cooperation agreement with the Government. Pursuant to the terms of that agreement, Monsegur pled guilty to a 12-count Superseding Information, S1 11 Cr. 666, charging him with nine counts related to computer hacking; one count related to credit card fraud; one count of conspiring to commit bank fraud; and one count of aggravated identity theft. In addition to resolving the charges brought against him in the Southern District of New York, Monsegur's guilty plea also resolved four cases filed against him in other districts (including the Eastern and Central Districts of California, the Northern District of Georgia, and the Eastern District of Virginia) which were transferred to the Court under docket numbers 11 Cr. 693-696, respectively.

On or about May 24, 2012, the Government moved to revoke Monsegur's bail because he made unauthorized online postings. Monsegur was arrested and remanded to custody the following day. He was released on a revised bail package on or about December 18, 2012, and has remained at liberty since that date. Accordingly, Monsegur has served approximately 7 months in prison in connection with this case.

In the PSR, Probation correctly calculates that the defendant's base offense level is 7 pursuant to U.S.S.G. §2B1.1(a)(1) and correctly applies a 22-level enhancement in light of a loss amount between $20 million and $50 million[4]; a 6-level enhancement given that the offense involved more than 250 victims; a 2-level enhancement for sophisticated means; and a 4-level enhancement given that the defendant was convicted of violating Title 18, United States Code, Section 1030(a)(5)(A). The defendant receives a three-level reduction for his acceptance of responsibility, resulting in a total adjusted offense level of 38. (PSR ¶¶ 43-59.) The defendant has zero criminal history points, and is therefore in Criminal History Category I. (PSR ¶¶ 60-66.)

Based on an offense level of 38 and a Criminal History Category of I, the defendant's advisory Guidelines Range is 235 to 293 months' imprisonment. (PSR ¶ 96.) In addition, absent the Court granting the Government's motion pursuant to Title 18, United States Code, Section 3553(e), the defendant would face a mandatory consecutive term of two years' imprisonment, resulting in a total advisory Guidelines range of 259 to 317 months' imprisonment.

III. Monsegur's Cooperation

Monsegur acknowledged his criminal conduct from the time he was first approached by agents, before he was charged in this case. Monsegur admitted both to prior criminal conduct about which the Government had not developed evidence, as well as his role in both Internet Feds and LulzSec. Monsegur subsequently and timely provided crucial, detailed information regarding computer intrusions committed by these groups, including how the attacks occurred,

[4] This loss figure includes damages caused not only by hacks in which Monsegur personally and directly participated, but also damages from hacks perpetrated by Monsegur's co-conspirators in which he did not directly participate. Monsegur's actions personally and directly caused between $1,000,000 and $2,500,000 in damages. Had Monsegur not candidly acknowledged his affiliation with the groups that committed the other hacks, his advisory Guidelines range likely would have been substantially lower.

which members were involved, and how the computer systems were exploited once breached. As set forth below, Monsegur's consistent and corroborated historical information, coupled with his substantial proactive cooperation and other evidence developed in the case, contributed directly to the identification, prosecution and conviction of eight of his major co-conspirators, including Hammond, who at the time of his arrest was the FBI's number one cybercriminal target in the world. On top of that, Monsegur engaged in additional, substantial proactive cooperation that enabled the FBI to prevent a substantial number of planned cyber attacks, as set forth below.

A. Monsegur's Acceptance of Responsibility

To begin with, Monsegur immediately admitted his role in Internet Feds and LulzSec, including his role in the major cyber intrusions set forth in the first section of this memorandum. In addition, Monsegur admitted to playing a role in cyber attacks and intrusions with these groups that the Government had not previously known that he played. For example, Monsegur admitted to participating in DDoS (Distributed Denial of Service)[5] attacks against the computer systems of PayPal, MasterCard, and Visa, among other targets. Monsegur also admitted to hacking certain government websites and taking government servers offline, to providing "security research" (that is, publicizing vulnerabilities in computer systems that others could exploit), and to using his "celebrity" hacker name – "Sabu" – in the hopes that it would inspire others to join certain criminal activities of these groups.

In addition to his admission to these crimes, Monsegur admitted to engaging in hacking activities about which the Government had not previously developed evidence. According to Monsegur, between 1999, when he first began hacking computers, and late 2003/early 2004,

[5] DDoS attacks involve the use of several computers to bombard a victim's computer system with connection requests, thereby overwhelming the victim's system, often resulting in the temporary shutdown of the victim's website.

Monsegur hacked into thousands of computers. For the next approximately two years, Monsegur identified vulnerabilities in perhaps 200 computer systems in an effort to grow a legitimate computer security firm. Then, starting around 2006, Monsegur hacked into computer systems for personal financial gain, or as part of hacker groups that broke into systems for a variety of reasons, including so-called "hacktivism." Monsegur admitted that, before joining Anonymous hacking crews, he hacked into a variety of websites and computer systems including the websites of several businesses. Through these hacks, Monsegur was able to steal credit card information, and then sold the credit card numbers, gave them away to family members and friends, and used them to pay his own bills. On at least one occasion, Monsegur was hired to hack into a business's computer system. He also successfully hacked into a business's website and had merchandise delivered to him free of charge.

Finally, Monsegur acknowledged a variety of other criminal conduct including sales and attempted sales of small quantities of marijuana; personal marijuana use; illegally possessing an unlicensed firearm; and purchasing stolen goods including electronics and jewelry.

B. Monsegur Assists Law Enforcement in Identifying and Locating LulzSec Members and Affiliates

Monsegur's primary substantial assistance came in the form of his cooperation against significant cybercriminals affiliated with Anonymous, Internet Feds, and LulzSec. He provided detailed historical information about the activities of Anonymous, contributing greatly to law enforcement's understanding of how Anonymous operates. Monsegur also provided crucial and detailed information about the formation, organization, hierarchy and membership of these hacking groups, as well as specific information about their planning and execution of many major cyber attacks, including the specific roles of his co-conspirators in committing those crimes. He also provided historical information that helped resolve open investigations into

several computer intrusions committed by members of Internet Feds and LulzSec, including the hacks identified above.

In addition to this crucial historical information, Monsegur proactively cooperated with ongoing Government investigations. Working sometimes literally around the clock, at the direction of law enforcement, Monsegur engaged his co-conspirators in online chats that were critical to confirming their identities and whereabouts. During some of the online chats, at the direction of law enforcement, Monsegur convinced LulzSec members to provide him digital evidence of the hacking activities they claimed to have previously engaged in, such as logs regarding particular criminal hacks. When law enforcement later searched the computers of particular LulzSec members, they discovered copies of the same electronic evidence on the individuals' computers. In this way, the online nicknames of LulzSec members were definitively linked to their true identities, providing powerful proof of their guilt. Other times, at the direction of law enforcement, Monsegur asked seemingly innocuous questions designed to elicit information from his co-conspirators that, when coupled with other information obtained during the investigation, could be used to pinpoint their exact locations and identities. Monsegur's substantial proactive cooperation, as set forth more particularly below, contributed directly to the identification, prosecution, and conviction of eight of his co-conspirators, including Hammond.

As disclosed in their communications, Hammond and certain other co-conspirators had learned how to exploit a particular software application vulnerability that enabled him to hack into many computer servers. At law enforcement direction, Monsegur attempted to learn how these targets were able to exploit this vulnerability, but was unsuccessful. At the same time, Monsegur was able to learn of many hacks, including hacks of foreign government computer servers, committed by these targets and other hackers, enabling the Government to notify the

victims, wherever feasible, so the victims could engage in remediation efforts and prevent further damage or intrusions.

Monsegur's cooperation was complex and sophisticated, and the investigations in which he participated required close and precise coordination with law enforcement officers in several locations. For instance, during the investigation of Hammond, Monsegur (who was then in New York) engaged in online chats with Hammond (who was then in Chicago), while coordinating with FBI agents in New York, physical surveillance teams deployed in Chicago, and an electronic surveillance unit in Washington, D.C.

Monsegur also engaged in a significant undercover operation in an existing investigation through which, acting at the direction of law enforcement, Monsegur gathered evidence that exposed a particular subject's role in soliciting cyber attacks on a foreign government. The evidence he enabled the Government to obtain was extremely valuable, and the Government could not otherwise have obtained it without his assistance. Although this cooperation has not resulted in any prosecutions to date, the Government believes his information, and the evidence he helped to obtain in this matter, is extremely significant.

C. Monsegur Assists Law Enforcement in Preventing Hacks

Notably, during the period of his cooperation, Monsegur received communications from hackers about vulnerabilities in computer systems, as well as computer hacks that were being planned or carried out by them. The FBI used this information, wherever feasible, to prevent or mitigate harm that otherwise would have occurred. The FBI estimates that it was able to disrupt or prevent at least 300 separate computer hacks in this fashion. The victims included divisions of the United States Government such as the United States Armed Forces (specifically, [redacted], the United States Congress, the United States Courts (specifically, [redacted]

[redacted]), and NASA; international intergovernmental organizations (specifically, [redacted]); and several private companies including a television network ([redacted]), a security firm ([redacted]), a video game manufacturer ([redacted]), and an electronics conglomerate ([redacted]). Although difficult to quantify, it is likely that Monsegur's actions prevented at least millions of dollars in loss to these victims.

Monsegur also provided information about vulnerabilities in critical infrastructure, including at a water utility for an American city, and a foreign energy company. Law enforcement used the information Monsegur provided to secure the water utility, and the information about the energy company was shared with appropriate government personnel. In addition, when Anonymous claimed to have hacked the electrical grid in the United States, Monsegur communicated with certain Anonymous members who revealed that the claims were a hoax. This saved the Government the substantial time and resources that otherwise would have been deployed in responding to these bogus claims.

Discussion

I. Applicable Law

The United States Sentencing Guidelines still provide strong guidance to the Court following United States v. Booker, 543 U.S. 220 (2005), and United States v. Crosby, 397 F.3d 103 (2d Cir. 2005). As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range" — that "should be the starting point and the initial benchmark." Gall v. United States, 128 S. Ct. 586, 596 (2007).

After that calculation, however, a sentencing judge must consider seven factors outlined in Title 18, United States Code, Section 3553(a): "the nature and circumstances of the offense and the history and characteristics of the defendant," 18 U.S.C. § 3553(a)(1); the four legitimate

purposes of sentencing, see id. § 3553(a)(2); "the kinds of sentences available," id. § 3553(a)(3); the Guidelines range itself, see id. § 3553(a)(4); any relevant policy statement by the Sentencing Commission, see id. § 3553(a)(5); "the need to avoid unwarranted sentence disparities among defendants," id. § 3553(a)(6); and "the need to provide restitution to any victims," id. § 3553(a)(7). See Gall, 128 S. Ct. at 596 & n.6.

II. Evaluation of Defendant's Cooperation

Section 5K1.1 of the Guidelines sets forth five non-exclusive factors that sentencing courts are encouraged to consider in determining the appropriate sentencing reduction for a defendant who has rendered substantial assistance, including the significance and usefulness of the assistance; the truthfulness, completeness and reliability of the defendant's information and testimony; the nature and extent of the assistance; any injury suffered, or any danger or risk of injury to the defendant or his family resulting from his assistance; and the timeliness of the assistance.

As to the significance and usefulness of the defendant's assistance, Monsegur's cooperation was extraordinarily valuable and productive. Monsegur provided unprecedented access to LulzSec – a tightly knit group of hackers who targeted and successfully breached a variety of computer systems operated by governments, businesses, and news media outlets. Through Monsegur's historical information and substantial proactive cooperation, the FBI and international law enforcement were able to pierce the secrecy surrounding the group, identify and locate its core members, and successfully prosecute them. In particular, when Monsegur first was arrested, he provided the FBI with information about the identities and whereabouts of core LulzSec members. This information helped focus the investigations being conducted by the FBI and international law enforcement, allowing them to develop additional evidence against

LulzSec members. At the direction of law enforcement, Monsegur then engaged in online chats with various LulzSec members, convincing them to disclose details that confirmed their identities and whereabouts including, as noted above, digital evidence that later was matched to files stored on the LulzSec members' computers. Monsegur also provided in-depth information regarding many of the computer hacks that LulzSec had perpetrated.

Monsegur's efforts contributed directly in the identification, prosecution, and convictions of core members of LulzSec, including:

- Ryan Ackroyd, a/k/a "Kayla." Ackroyd was arrested by authorities in the United Kingdom. He pled guilty and was sentenced to 30 months' imprisonment.

- Jake Davis, a/k/a "Topiary." Davis was arrested by authorities in the United Kingdom. He pled guilty and was sentenced to 24 months' custody in a young offender institution.

- Mustafa Al-Bassam, a/k/a "T-Flow." Al-Bassam was arrested by authorities in the United Kingdom. He pled guilty and was sentenced to a 20 month term, which was suspended for two years, as well as 300 hours' community service.

- Darren Martyn, a/k/a "pwnsauce," was arrested by authorities in Ireland. He subsequently pled guilty and received a sentence of probation and a fine.

In addition to these core members of LulzSec, Monsegur's cooperation led to the arrest and prosecution of others who contributed to LulzSec's hacking efforts, including:

- Jeremy Hammond, a/k/a "Anarchaos." As the Court is aware, Hammond, the FBI's most wanted cybercriminal in the world at the time of his arrest, was prosecuted in the Southern District of New York, pled guilty, and was sentenced by the Court principally to a term of imprisonment of 120 months.

- Ryan Cleary. Cleary was arrested by authorities in the United Kingdom. He pled guilty and was sentenced to 32 months' imprisonment.

- Donncha O'Cearrbhail, a/k/a "palladium." O'Cearrbhail was arrested by authorities in Ireland, pled guilty, and was sentenced to probation and a fine.

- Matthew Keys. Keys is currently charged in the Eastern District of California in connection with his role in permitting unauthorized access to the Tribune Company's computer systems.

All of these prosecutions were extremely important to the Government. As set forth above, these hackers engaged in significant cyber attacks against computer systems that belonged to government agencies and contractors, news media outlets, non-profit institutions, and private entities. Some of the attacks defaced news media websites, others rendered government websites inaccessible, and still others resulted in the exfiltration of the personal identification information of victims.

Yet the number of prosecutions to which Monsegur contributed only partially conveys the significance and utility of his cooperation. On a daily basis throughout the summer of 2011, Monsegur provided, in real time, information about then-ongoing computer hacks and vulnerabilities in significant computer systems. Through Monsegur's cooperation, the FBI was able to thwart or mitigate at least 300 separate hacks. The amount of loss prevented by Monsegur's actions is difficult to fully quantify, but even a conservative estimate would yield a loss prevention figure in the millions of dollars. Moreover, Monsegur provided information about actual and purported vulnerabilities in critical infrastructure, allowing law enforcement to respond appropriately.

Finally, as set forth above, Monsegur engaged in a significant undercover operation in which, acting at the direction of law enforcement, he helped to obtain evidence that exposed a subject's role in soliciting cyber attacks on the computer systems of a foreign government. While it has not resulted in prosecutions to date, this evidence is significant and valuable to the Government.

As to Monsegur's truthfulness, completeness and reliability, he presented as fully candid, and admitted not only to crimes about which the Government had gathered evidence, but also crimes about which the Government had not previously gathered evidence. Monsegur's information was also consistently reliable and complete, corroborated by documents and electronic files, as well as by statements from other witnesses. As noted above, while Monsegur made certain unauthorized online postings that resulted in the revocation of his bail and his incarceration for several months, following his release from custody in December 2012, Monsegur made no further unauthorized postings.

As to the nature and extent of Monsegur's cooperation, as noted above, Monsegur has been cooperating with law enforcement for approximately three years. His cooperation entailed many multi-hour meetings with FBI agents that extended into the late evening and early morning hours. Monsegur provided substantial historical cooperation, as well as substantial proactive cooperation, and he was prepared to testify if needed. However, to date, every defendant against whom Monsegur has cooperated has pled guilty with the exception of Keys, who is awaiting trial. Monsegur's cooperation no doubt played a significant role in securing several of these guilty pleas in that, among other things, acting at the direction of law enforcement, Monsegur obtained incriminating online chats with most of the defendants that constituted strong proof of each defendant's guilt.

The nature of Monsegur's cooperation was also somewhat atypical in that his work as a cooperating witness was made public shortly after the arrest of the core LulzSec members. This revelation in itself served an important deterrent effect throughout the hacking community. At the same time, it resulted in significant scrutiny of Monsegur and his family members.

As to the danger or risk associated with Monsegur's cooperation, Monsegur faced hardships because of his cooperation. During the course of his cooperation, the threat to Monsegur and his family became severe enough that the FBI relocated Monsegur and certain of his family members. Monsegur repeatedly was approached on the street and threatened or menaced about his cooperation once it became publicly known. Monsegur was also harassed by individuals who incorrectly concluded that he participated in the Government's prosecution of the operators of the Silk Road website.

Moreover, Monsegur has been vilified online by various groups affiliated with the Anonymous movement, which particularly affected him given the central role that his online activity played in his life prior to his cooperation with the Government. Among other things, certain groups have sought to release Monsegur's personal identification information (such as his exact address) as well as the personal identification information of certain of his family members.

Members of Monsegur's family have been threatened because of his cooperation, and one of those relatives was involved in a physical altercation regarding Monsegur's cooperation. Monsegur's family members have also repeatedly been approached by members of the media. In one instance, a reporter was removed from the school of the children for whom Monsegur served as guardian after the reporter entered the school and attempted to interview the children.

As to the timeliness of Monsegur's assistance, as noted above, he immediately cooperated with law enforcement. Just hours after being approached by law enforcement, he was back online cooperating proactively. His timely decision to cooperate helped prevent or mitigate hundreds of hacks; allowed the Government to develop sufficient evidence to charge multiple individuals with serious computer crimes; and revealed a significant subject's role in soliciting cyber attacks against a foreign government. Had Monsegur delayed his decision to cooperate, his efforts would have been far less fruitful. In fact, LulzSec had developed an action plan to destroy evidence and disband if the group determined that any of its members had been arrested, or were out of touch with the other group members for an extended period of time. Accordingly, had Monsegur delayed his decision to cooperate and remained offline for an extended period of time, it is likely that much of the evidence regarding LulzSec's activities would have been destroyed, and members of the group would have become much more difficult to locate. Monsegur's immediate decision to cooperate was thus particularly important to the ultimate successes that stemmed from his cooperation.

Conclusion

In light of the foregoing facts, the Government respectfully requests that, pursuant to Section 5K1.1 of the Guidelines, the Court grant the defendant a substantial downward departure at sentencing. In addition, the Government respectfully moves, pursuant to Title 18, Section 3553(e), for relief from the otherwise applicable mandatory minimum sentence in this case. Such a sentence will appropriately account for the defendant's extraordinary cooperation, and be sufficient, but not greater than necessary, to serve the legitimate goals of sentencing.

Request to Seal

The Government respectfully requests that it be permitted to file limited portions of this submission under seal to protect the identities of certain victims.

Dated: New York, New York
May 23, 2014

Respectfully submitted,

PREET BHARARA
United States Attorney

By: /S/
James J. Pastore, Jr.
Assistant United States Attorney
Tel.: (212) 637-2418