UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA v. MARCEL LEHEL LAZAR a/k/a "GUCCIFER" a/k/a "GUCCIFER SEVEN" a/k/a "MICUL FUM" a/k/a "MARCEL LAZAR LEHEL" Defendant.	Criminal No. 1:14-cr-213 Honorable James C. Cacheris Sentencing: September 1, 2016

GOVERNMENT'S POSITION ON SENTENCING

Beginning in October 2012, defendant Marcel Lehel Lazar embarked on a fourteen-month computer hacking spree during which he broke into the personal email accounts of at least one hundred Americans. Many of his victims were public figures whom he targeted for their high profile. Other victims were private citizens whom he selected simply because they appeared on the email contact list of another victim. Regardless of their stature, for almost all of his victims defendant illegally copied private information that he found in their accounts. The confidential information that defendant stole included personal email correspondence, medical records, financial documents, intimate photographs, and personally identifying information. Defendant also impersonated some of his victims online, using their accounts to harass and embarrass them and to help him collect information about other unsuspecting targets. In a nightmare come true for his victims, defendant released their personal information to multiple online media entities, who in turn featured stories about his victims and made publicly available the online storage drives where defendant had uploaded his stolen information.

At the time of his offense conduct, defendant was on probation in Romania for a 2011 conviction for computer hacking. Undeterred by his prior conviction, defendant waited less than a year to re-offend. He changed remarkably little about the execution of his hacking scheme: he targeted celebrities and broke into private accounts by correctly guessing passwords or re-setting them. This time, however, to elude law enforcement, defendant chose a new pseudonym – "Guccifer" – and employed proxy servers in Russia to mask his true location and throw anyone tracing his Internet Protocol (IP) address off the scent. Notably, defendant's victims were not extended any similar considerations to protect their identities. At the end of 2013, when defendant feared that he had been discovered, he demolished his computers and phones with an ax in the hopes that he would destroy evidence.

For his crimes, defendant has pleaded guilty to one count of aggravated identity theft under 18 U.S.C. § 1028A, and one count of unauthorized access to a protected computer under 18 U.S.C. § 1030(a)(2)(C). A conviction for aggravated identity theft carries a mandatory two-year sentence that must be served consecutively to any other sentence defendant might receive. The determination of defendant's sentence for unauthorized computer access must consider the appropriate Sentencing Guidelines range and the sentencing factors in 18 U.S.C. § 3553(a).

On defendant's Guidelines range, the government respectfully submits that an upward departure on defendant's criminal history category is warranted due to defendant's prior convictions in Romania (which are otherwise not counted because they are foreign convictions). An upward departure from Criminal History Category I to II will avoid the substantial underrepresentation of defendant's criminal history. At Criminal History Category II and an offense level of 16, defendant's Guidelines range is 24-30 months. The government submits that a sentence at the high-end of this Guidelines range for defendant's computer hacking offense

would be sufficient, but not more than necessary, to satisfy the § 3553 factors, which would be added to the two-year sentence under § 1028A to arrive at defendant's final imprisonment term.

BACKGROUND

Defendant is a 44-year-old Romanian citizen and native. Five years ago, he was charged in Romania with illegally accessing dozens of email and Facebook accounts belonging to Romanian celebrities. PSR ¶¶ 22, 81. He was also charged with publicly releasing private communications that he had lifted from these accounts. *Id.* ¶ 81. Although defendant published his exploits under the pseudonym "Micul Fum" – translated to "Little Smoke" – he was caught and ultimately convicted in Romania of unauthorized access to a computer system. *Id.* ¶¶ 22, 81. In March 2012, he was given a three-year sentence, all of it suspended, and six years of probation. *Id.* ¶ 81.

Undeterred, by the fall of 2012 defendant decided to again hack into celebrities' personal accounts. PSR ¶ 16. This time he focused on Americans. From at least October 2012 through January 2014, defendant – working under a new moniker he'd created, "Guccifer" – went on what has been described as a "rampage through the email accounts of rich and powerful Americans."[1] But defendant didn't discriminate: he also hijacked personal email accounts belonging to private citizens. *Id.* ¶¶ 30, 36. In some instances, defendant victimized the children, spouses, and friends of other victims. PSR ¶¶ 28-29, 56 (at 14). To trawl for new targets, defendant frequently emailed contacts on a victim's contact list while impersonating that victim. *Id.* ¶ 27. In addition, defendant sometimes hunted down his victims' Facebook accounts,

[1] Andrew Higgins, "For Guccifer, Hacking Was Easy. Prison Is Hard," *New York Times* at A1 (Nov. 10, 2014), available at http://www.nytimes.com/2014/11/11/world/europe/for-guccifer-hacking-was-easy-prison-is-hard-.html (attached as Exhibit A).

illegally gained access to them, and defaced them. *Id.* ¶¶ 33-34. All told, at least one hundred Americans lost control of their personal online accounts to defendant. *Id.* ¶¶ 22-25.

Defendant also subjected particular victims to a campaign of harassment. For Victim 3 in the indictment, once the defendant gained entry into his Facebook account, defendant posted outrageous comments to the victim's public-facing site. PSR ¶ 34. Defendant also launched an email from Victim 3's account to dozens of media organizations that contained similarly provocative messages. *Id.* ¶ 35. Going even further, defendant then broke into another victim's Facebook and email accounts and, from that account, bombarded Victim 3 with messages and links to online drives where defendant had stored Victim 3's stolen information. *Id.* ¶¶ 40-41.

Furthering the harm to his victims, over the course of his hacking "rampage" defendant released his victims' personal information and private communications to online media outlets, who in turn published portions of this confidential information. PSR ¶¶ 18, 31, 35, 42, 46; *id.* at 29 (Victim Impact Statement). The defendant used Google Drive, an online file storage service provided by Google, Inc., to upload and save the voluminous and illegal fruits of his hacking labor. *Id.* ¶¶ 38, 40, 47. He called this collection of Google Drives the "Guccifer Archive." *Id.* ¶¶ 47. In December 2013, the defendant provided access to the Guccifer Archive to two online entities that publish documents on their sites, and to which defendant had previously provided stolen material. *Id.* ¶ 47. One of these entities then published a story based on the contents of the storage drives that included a list of previously unknown victims. The other posted links to the Guccifer Archive. *Id.* ¶¶ 42, 47, 49-50. As a result, defendant's full repository of hacked information that he had methodically saved over the fourteen months – private email correspondence, medical information, financial information, photographs, personal identifying information, and other private property – was made available to the public.

To conceal his true identity and location, defendant committed his unlawful intrusions using proxy servers located in other countries, including Russia. PSR ¶¶ 21, 29, 33, 45, 82. At the end of 2013, defendant, fearing that law enforcement might have unmasked his identity, panicked and used an ax to destroy the computer devices and phone that he had used to break into his victims' accounts, and buried the remains in his backyard. *Id.* ¶ 33, 82 (at 20).

Defendant was initially arrested in Romania for his computer hacks against Romanians. In the summer of 2013, defendant broke into the personal email accounts of a Romanian politician (a former member of the European Parliament) and the then-head of the Romanian intelligence service. PSR ¶ 82. Once he took over the Romanian politician's email account, he reset her password, read her email messages, copied them onto his personal computer, and then transmitted these private messages to online sites for publication. *Id.* ¶ 82. Defendant went even further once he got into the personal email account of the Romanian intelligence officer: he contacted the victim via email, relayed that he had accessed the victim's private information, and suggested "an exchange" for something the defendant had not yet decided on. *Id.* ¶ 82. When the victim did not respond, defendant sent screenshots of the victim's emails to several TV stations and newspapers. *Id.* ¶ 82.

With help from U.S. investigators, Romanian law enforcement identified defendant and arrested him on January 22, 2014. PSR ¶¶ 52, 82. He was convicted of unauthorized access to a computer system; unauthorized altering of data from a computer system; unauthorized transfer of data from a computer system; and violation of private correspondence secrecy. *Id.* ¶ 82. In June 2014, defendant was given a four-year sentence. Since the defendant had been on probation at the time of his crimes, his prior three-year sentence for his 2011 hacking conduct was reinstated, resulting in a total seven-year sentence in Romania. *Id.* ¶¶ 52, 82.

On June 12, 2014, a grand jury in the Eastern District of Virginia returned a nine-count indictment charging defendant for his hacking crimes against American victims. The indictment charged him with wire fraud, unauthorized computer access, aggravated identity theft, cyberstalking, and obstruction of justice. ECF No. 1 (Indictment). On March 31, 2016, defendant was temporarily surrendered to the United States from Romania, where he was still serving his Romanian sentence, to face the charges in the indictment. PSR ¶ 6. He has been in U.S. Marshals' custody since April 1, 2016.

On May 25, 2016, the Court accepted defendant's plea of guilty to Counts Five and Seven of the indictment, which respectively charged him with unauthorized access to a protected computer (in violation of 18 U.S.C. § 1030(a)(2)(C)) and aggravated identity theft (in violation of 18 U.S.C. § 1028A(a)(1)). ECF No. 28 (Plea Agreement).

SENTENCING ANALYSIS

I. Conviction for aggravated identity theft (18 U.S.C. § 1028A)

Defendant is subject to a mandatory two-year sentence for his offense of aggravated identity theft. This required sentence must be served consecutively to any sentence that the Court imposes for defendant's offense of unauthorized access to a computer. *See* 18 U.S.C. § 1028A(a)-(b). Convictions for aggravated identity theft are not subject to analysis under the Sentencing Guidelines, and thus the Guidelines' provisions regarding offense-level adjustments and criminal history calculation do not apply. U.S.S.G. § 2B1.6; PSR ¶ 67 n.2. The Guidelines' sentence is simply the term of imprisonment required by the statute. Accordingly, defendant must be sentenced to a two-year term of imprisonment for his aggravated identity theft offense, which must run consecutively to any sentence he receives for his computer hacking offense.

II. Conviction for unauthorized access to a protected computer (18 U.S.C. § 1030)

To determine the appropriate sentence for defendant's offense of unauthorized access to a computer, the Court must consult both the Sentencing Guidelines and the sentencing factors in 18 U.S.C. § 3553(a). Although the Sentencing Guidelines are advisory, district courts are required to "consult those Guidelines and take them into account when sentencing." *United States v. Booker*, 543 U.S. 220, 264 (2005). Under the required procedures, a "district court shall first calculate (after making the appropriate findings of fact) the range prescribed by the guidelines. Then, the court shall consider that range as well as other relevant factors set forth in the guidelines and those factors set forth in [18 U.S.C.] § 3553(a) before imposing the sentence." *United States v. Hughes*, 401 F.3d 540, 546 (4th Cir. 2005) (citation omitted).

A. Application of Sentencing Guidelines

While the government agrees with the PSR's calculation of defendant's Guidelines offense level at 16, the government submits that, given defendant's prior hacking crimes in Romania – and the fact that he was on probation when he committed the current offense – an upward departure on criminal history is warranted. Applying an upward departure from Criminal History Category I to II, defendant's Guidelines range for his hacking offense is 24-30 months.

Offense level. The PSR's calculation of defendant's total offense level mirrors the joint recommendation in defendant's plea agreement. PSR ¶¶ 7, 68-79. As reflected in the PSR and plea agreement, defendant's total offense level for his crime of unauthorized access to a computer is calculated as follows:

Guideline	
Base offense level (Section 2B1.1(a)(2))	6
10 or more victims (Section 2B1.1(b)(2)(A)(i))	+2
Substantial part of a fraudulent scheme was committed from outside of the United States; and/or the offense involved sophisticated means (Sections 2B1.1(b)(10)(B), (C))[2]	+4
Offense involved intent to obtain personal information and the offense involved the unauthorized public dissemination of personal information (Section 2B1.1(b)(17)(A), (B))	+2
Victims of the offense include former government officers or employees and the immediate family of former government officers and employees (Section 3A1.2(a)(B))	+3
Defendant willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice (Section 3C1.1)	+2
Acceptance of responsibility (Section 3E1.1)	-3
TOTAL OFFENSE LEVEL	**16**

Given the defendant's timely acceptance of responsibility, the government moves the Court for a one-level reduction under U.S.S.G. § 3E1.1(b), as reflected in the chart above, which the Probation Office has appropriately included in its calculations. *Id.* ¶ 77-78.

Criminal history. Defendant's criminal convictions in Romania, by virtue of being foreign convictions, are excluded from the computation of defendant's criminal history category. *See* U.S.S.G. § 4A1.2(h); PSR ¶¶ 81-82. The PSR thus assigns defendant, who has no prior convictions in the United States, zero criminal history points, resulting in a criminal history category of I. *Id.* ¶¶ 83-84. The Guidelines expressly recognize, however, as does the PSR, that an upward departure on criminal history category "may be warranted based on . . . [a] previous

[2] The offense level must be increased by 4 levels to reach offense level 12.

foreign sentence for a serious offense." U.S.S.G. §4A1.3 note 2; *see id.*§4A1.3(a)(2); PSR ¶ 111.

Defendant's foreign criminal history presents a textbook example of when an upward departure is appropriate. The assignment of zero criminal history points to defendant renders nonexistent his 2011 conviction for computer hacking – an offense almost identical to the one he committed in this case. That offense was serious enough that he received a three-year sentence, which he was ordered to serve in January 2014. PSR ¶ 81. Of equal significance, excluding his Romanian criminal history excludes the fact that defendant was on probation when he committed his more recent hacking spree. The failure of defendant's criminal history category to otherwise reflect his status as a recidivist who, in abject disregard of his sentence, waited less than a year to re-commit the same crimes, "substantially underrepresents the seriousness of the defendant's criminal history" and "the likelihood that the defendant will commit other crimes." U.S.S.G. § 4A1.3(a)(1).

The government submits that an upward departure from Criminal History Category I to II would therefore be appropriate. The extent of an upward departure is determined "by using, as a reference, the criminal history category applicable to defendants whose criminal history or likelihood to recidivate most closely resembles that of the defendant's." U.S.S.G. § 4A1.3(a)(4)(A). Under this analysis, treating defendant's 2011 conviction and three-year sentence as a domestic and not foreign punishment would boost defendant's criminal history points to 3. Alternatively, if defendant's 2011 sentence is viewed as a suspended sentence that collects no criminal history points, defendant would receive 2 points because he committed the current offense while on probation.[3] *See* U.S.S.G. § 4A1.1(a), (d). Under either scenario,

[3] Defendant's 2014 convictions and sentence should likely receive no points under this analysis, since treating them as domestic offenses would merge them with the current offense, albeit with different victims.

defendant's criminal history would ratchet up to Category II, resulting in an appropriate Guidelines sentencing range of 24-30 months.

B. Application of Section 3553 Factors

The Section 3553 factors that the Court must consider in determining defendant's sentence for computer hacking underscore the need for a significant sentence in this case.[4] For the reasons that follow, the government submits that a sentence at the high-end of the Guidelines range for the computer hacking offense would be sufficient and not greater than necessary to satisfy the statutory factors.

1. The nature and circumstances of defendant's crimes warrant a significant sentence.

By any measure, the sheer scope of defendant's hacking activities – and the huge volume of private information he subsequently stole and made publicly available – warrants a significant sentence in this case.

Over the fourteen-month period that defendant went on his hacking rampage, he amassed at least 100 victims in the United States. PSR ¶ 23. Notably, the 100-victim figure substantially underrepresents the actual scope of defendant's conduct in this case. It does not, for instance,

[4] Title 18, United States Code, Section 3553(a) provides: "The court shall impose a sentence sufficient, but not greater than necessary, to comply with the purposes set forth in paragraph (2) of this subsection. The court, in determining the particular sentence to be imposed, shall consider -- (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need for the sentence imposed -- (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (B) to afford adequate deterrence to criminal conduct; (C) to protect the public from further crimes of the defendant; and (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range established for -- (A) the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines . . . (5) any pertinent policy statement . . . (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and (7) the need to provide restitution to any victims of the offense."

account for the large number of defendant's victims from other countries. In 2013, defendant targeted not just American victims, but also victims in Romania and, in his words, "Asia Minor, where I looked for and found ambassadors' accounts." March 2014 Interview (attached as Exhibit B) at 5. Nor does that number reflect the scores of unsuccessful hacking attempts defendant made. By defendant's own estimate, his "success rate" at gaining entry to private accounts was only 8-10% of his attempts. Exhibit B at 4.

In selecting and targeting new victims, defendant used fraud, identity theft, and even engaged in harassment campaigns against victims. Often he selected future victims by raiding the email contact lists of individuals whose accounts he had already compromised. PSR ¶ 27. In using this hopscotch approach, defendant frequently impersonated a victim to communicate with others on that victim's contact list. *Id.* ¶ 27. In addition, once the defendant broke into a victim's email account, he often took additional steps to maintain exclusive control over that account, such as by changing the password or answers to the security questions. *Id.* ¶ 25. With Victim 3, defendant subjected him to repeated taunts and harassing behavior. *Id.* ¶¶ 32-42.

Not satisfied with simply gaining access to his victims' accounts, defendant furthered the harm to his victims by releasing the contents of their private communications to media organizations, who then published the stolen information. Defendant's criminal conduct against Victim 1 is illustrative. Defendant's seemingly obsessive quest to break into the private online accounts of public figures took off in December 2012, when he successfully hacked into – and then repeatedly accessed – the personal email account of Victim 1, an immediate family member of two former U.S. presidents. PSR ¶¶ 28-29. Defendant brazenly looted Victim 1's private communications, confidential medical information, photographs, and personal identifying information, and transmitted this stolen information to multiple media organizations. *Id.* ¶¶ 29-

31. As a direct result, Victim 1's private information – along with that of her family members – was published online without her consent. *Id.* ¶ 31.

Certainly defendant's preferred victims were high-profile Americans – individuals with media cachet. In his own words, he was mostly interested in "celebrities." Exhibit B at 3. Thus, his victims included TV and movie actors, established journalists, elected officials, military leaders, and best-selling authors. PSR ¶ 56. But defendant also had no qualms in hijacking personal email accounts belonging to Americans with no public profile – businesspersons, civil servants, private citizens. Some were targeted simply because they were family members or friends of other victims. *Id.* ¶¶ 30-31, 56.

One of the victim impact statements submitted with the PSR illustrates the emotional trauma caused by defendant's deep invasion of privacy and utter disregard of consequences for his victims in releasing their private information to the media. PSR at 32-34. In or around July 2013, defendant broke into that victim's email account, peered through his private documents, and bundled up over a dozen pages of information he'd found that contained, among other things, sexually explicit emails and photographs. Defendant sent this packet of documents to an Internet gossip site that promptly published some of this information, along with the victim's name. Exhibits C, D (under seal). The unauthorized release of this "intensely embarrassing & humiliating" information on a public site caused the victim immense distress. PSR at 33. Although this incident occurred over three years ago, the victim's released information still remains on the site, which appears as a search result when the victim's name is searched using an online search engine. *Id.* at 33. The victim has no confidence that he will ever recover from the reputational harm caused by defendant's criminal conduct.

The extent of the harm caused by defendant's conduct is incalculable, as victims' private information continues to swirl around the internet. Defendant, in addition to cherry-picking stolen records to share with the public, also made enormous swaths of his victims' private information available online in one fell swoop by giving two online entities complete access to what he called the "Guccifer Archive." These multiple Google Drive accounts contained volumes of information that he had methodically copied from victims' email accounts, including personally identifying information, medical records, financial documents, private email correspondence, and full details of contact lists. PSR ¶ 47. Defendant set the controls of these online accounts to be publicly accessible. One of the online entities that defendant contacted published a story in January 2014 based on the contents of defendant's stolen information, that included mentions of victims not previously known. *Id.*¶ 49; see Exhibit E.[5] In December 2014, the other online entity published links to the Guccifer Archive to its site, for all the world to download. PSR ¶¶ 49-50.

Finally, defendant's destruction of evidence in this case further warrants a significant sentence. To thwart law enforcement, defendant destroyed the computer devices and phones he used to carry out his hacking scheme. PSR ¶ 48. He also used sophisticated means, including hiding his IP address, to avoid detection for over a year while his criminal exploits continued. A significant sentence would hold defendant accountable for his obstructive acts.

2. The defendant's history and characteristics warrant a significant sentence.

Defendant, as a repeat offender in such a short time period, has shown no respect for the law. Moreover, the fact that he derived gratification from controlling and releasing other parties'

[5] The Smoking Gun, "'Guccifer Files Further Detail Hacking Spree," Jan. 6, 2014, available at http://www.thesmokinggun.com/documents/guccifer-archive-687543 (attached as Exhibit E).

private information makes it more likely that he will re-offend in the future. A significant sentence is thus warranted.

Without a doubt, defendant knew that his conduct was illegal. Not only had defendant been previously charged and convicted of computer hacking on the basis of nearly identical behavior – illegally accessing the personal email and Facebook accounts of celebrities – but he took steps to avoid detection by using proxy servers to hide his true location. PSR ¶¶ 21, 29, 33, 45, 82. He also employed the pseudonym "Guccifer" online. When he believed that law enforcement had unmasked his identity, he axed his laptops and phone. Yet, despite knowing that he was again committing crimes for which he could be prosecuted, he continued to amass victims at a near-obsessive rate until he was arrested.

There can also be little doubt that defendant was motivated by the personal gratification he derived from controlling his victims' private information, and from receiving media attention. He was in it for himself, as he told law enforcement during a March 2014 interview:

> Question: Did you continue to gather information [after January 2013 hacks]?
>
> Answer: Yes, I was interested in the people, usually celebrities.
>
> Question: Were you interested in something that would be the topic of news, or something that would put them in embarrassing situations?
>
> Answer: No, I was looking for something that would serve my interests.

Exhibit B at 3.

Defendant, bragging about his exploits, reveled in self-glory. He particularly enjoyed boasting that he had not been caught. In February 2013, a website that had interviewed defendant reported: "The hacker contends that 'The feds' began investigating him a 'long time ago,' and that he has hacked 'hundreds of accounts.' Asked if he was concerned about the

FBI/Secret Service investigation that will no doubt follow shortly, he replied cryptically, 'i have an old game with the fucking bastards inside, this is just another chapter in the game.'"[6] The following month, the same website reported about defendant: "The hacker also mocked the criminal probe […]. 'i can figure out the feds have a finger up their ass; haha.' 'Guccifer' added, 'AND TELL THE FUCKING BASTARDS THAT…I NEVER STOP!'"[7] Defendant's display of arrogance continued, as reported by the press: "Asked whether he thought law enforcement was closing in, Guccifer replied, 'NO I am not concerned, i think i switch the proxies go to play some backgammon on yahooo watch tv, play with my family and my daughter.'" Exhibit A at 3. Indeed, even after defendant was captured by law enforcement, he could not help continuing to boast to the press – even when his boasts were lies. Shortly after defendant arrived in the United States to face the current charges, he bragged to a news outlet that he had gained unauthorized access to a presidential candidate's personal email server: "For me, it was easy," he said.[8]

Although defendant has accepted responsibility for his conduct, fundamentally he has shown no remorse for his crimes or concern for his victims. He has expressed no remorse for making so much of his victims' personal information publicly available. He certainly knew there would be consequences to his victims, as stated in a March 2014 interview:

---

[6] The Smoking Gun, "Audacious Hack Exposes Bush Family Pix, E-Mail," Feb. 7, 2013, available at http://thesmokinggun.com/documents/bush-family-hacked-589132.

[7] The Smoking Gun, "Colin Powell Facebook Page Was Hacked By Same Perp Who Broke Into Bush Family E-Mail Accounts," Mar. 11, 2013, available at http://thesmokinggun.com/buster/colin-powell-guccifer-facebook-hack-467842.

[8] http://www.foxnews.com/politics/2016/05/04/romanian-hacker-guccifer-breached-clinton-server-it-was-easy.html; *but see* Fox News Insider, "Comey: Hacker 'Guccifer' Lied About Accessing Clinton's Emails" (July 7, 2016), available at http://insider.foxnews.com/2016/07/07/comey-hacker-guccifer-lied-about-accessing-clintons-emails.

Question: Did you carefully consider the consequences of your actions as well?

Answer: Yes, they involved other people's lives as well.

Exhibit B at 3. Defendant knew but simply did not care.

Of deep concern is that defendant has implied that he was justified in hacking his victims. In a November 2014 interview with the press, defendant, reflecting on his conduct, stated: "What I did was right, of course." Exhibit A at 5. In a March 2016 interview, defendant characterized his crimes as an "achievement":

Agent: If you could go back to…

Defendant: 2013, 2012…

Agent: Yeah…and talk to Guccifer back then, what would you say to him?

Defendant: I'd say, "Alright, you have done a good job." Yeah. Because I was learning and improving in motion. I was making better and better steps. Maybe it's about a 50% achievement. It's good. Probably I say that. … What I've achieved is probably 50% of what I could have achieved.

March 2016 interview (audio clip attached as Exhibit F). For defendant, his hacking exploits of at least 100 American victims are worthy of celebration – which strongly suggest that defendant will again re-offend.

3. A significant sentence reflects the seriousness of defendant's crimes, promotes respect for the law, provides just punishment, affords adequate deterrence, and is consistent with sentences in other cases.

A sentence at the high-end of the Guidelines Range would address the seriousness of defendant's crimes and provide just punishment. It would also help address any false perception that unauthorized access of a computer is ever justified or rationalized as the cost of living in a wired society – or even worse, a crime to be celebrated. As one of defendant's victims noted in a newspaper opinion piece two years ago, defendant has received some online acclaim for his

crimes, which perpetuates the utter disregard to his victims of the consequences they must endure for privacy violations they never invited.[9] A significant sentence would counter that perverse narrative and bring a measure of justice to these victims.

Moreover, as incidents of computer hacking continue to rise, sentences in cases such as this gain increasing importance for their deterrent value. Defendant has not been sentenced yet and already another hacker or set of hackers who released private information online have branded themselves "Guccifer 2.0" in homage to defendant.[10] Given the anonymity available online and the proliferation of tools available to cybercriminals to evade law enforcement, significant penalties are necessary to send a message that hacking will not go unpunished.

Other courts have imposed substantial sentences for crimes similar to defendant's. Four years ago, a district court in California imposed a ten-year sentence on a defendant who, like the defendant in this case, illegally accessed the private email accounts of celebrities by guessing their account passwords or answers to their security questions. *See United States v. Chaney*, No. 2:11CR958 (C.D. Cal. Dec. 17, 2012). That defendant also pilfered through his victims' contact lists to identity additional victims. *Chaney*, ECF No. 32 ("Amended Plea Agreement") at 12 (attached as Exhibit H). That defendant also used a proxy service to conceal his true IP address. Exhibit H at 14. That defendant also forwarded the private information he stole from his victims to online media sites, and he acted without any financial incentive. Exhibit H at 14. While the victims in that case lost control over nude and sexually explicit photographs they had

---

[9] Diane McWhorter, "Stop Glorifying Hackers," *New York Times* at SR7 (Mar. 9, 2014), available at http://www.nytimes.com/2014/03/09/opinion/sunday/stop-glorifying-hackers.html (attached as Exhibit G).

[10] *See* http://www.nbcnews.com/tech/tech-news/7-things-you-didn-t-know-about-guccifer-2-0-n631166 ("'[Defendant] inspired me and showed me the way.'").

maintained, the victims in this case have similarly lost any measure of privacy over the information that defendant stole and caused to be publicly available. The damage to defendant's victims compels the need for a just punishment that accounts for the full measure of his crimes, while sending a deterrent message to others who would think to imitate him.

CONCLUSION

For the reasons stated above, the government respectfully submits that a sentence of two years for defendant's aggravated identity theft offense, and a sentence at the high-end of the adjusted Guidelines range of 24-30 months for the offense of unauthorized access to a protected computer, to run consecutively, is sufficient but not greater than necessary under 18 U.S.C. § 3553(a). The government also respectfully requests that a restitution order be entered in the amount of $1,300, payable to victims whose names will be submitted under seal.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s/

Maya D. Song
Jay V. Prabhu
Assistant United States Attorneys
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
Tel: (703) 299-3700
Fax: (703) 299-3981
maya.song@usdoj.gov
jay.prabhu@usdoj.gov

Peter V. Roman
Ryan K. Dickey
Senior Counsel, U.S. Department of Justice
Criminal Division
Computer Crime and Intellectual Property Section

CERTIFICATE OF SERVICE

I hereby certify that on August 26, 2016, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will automatically generate a Notice of Electronic Filing to the following counsel of record:

Shannon Quill
Cadence Mertz
Assistant Federal Public Defenders
Eastern District of Virginia
1650 King Street, Suite 500
Alexandria, VA 22314
shannon_quill@fd.org
cadence_mertz@fd.org

Counsel for defendant Marcel Lehel Lazar

I have provided a copy of the foregoing document via electronic delivery to:

Tracey M. White
United States Probation Officer
401 Courthouse Square, 3rd Floor
Alexandria, VA 22314
Tracey_white@vaep.uscourts.gov

By: /s/
Maya D. Song
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
Ph: (703) 299-3700
Fax: (703) 299-3981
maya.song@usdoj.gov