ANDRÉ BIROTTE JR.
United States Attorney
ROBERT E. DUGDALE
Assistant United States Attorney
Chief, Criminal Division
STEPHANIE S. CHRISTENSEN (SBN 236653)
Assistant United States Attorney
Cyber and Intellectual Property Crimes Section
JENNIFER L. WILLIAMS (SBN 268782)
OCDETF Section
United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-2400
Facsimile: (213) 894-0140
E-mail: stephanie.chritensen@usdoj.gov
jennifer.williams6@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. LUIS MIJANGOS, Defendant.	CR No. 10-743-GHK GOVERNMENT'S OBJECTIONS TO THE PSR AND SENTENCING POSITION

Plaintiff, United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, hereby files its Objections to the PSR and Sentencing Position.

This document is based upon the attached memorandum of points and authorities and exhibits thereto (including those filed concurrently hereto under seal), the Presentence

Investigation Report, and any other evidence or argument that the Court may wish to consider at the time of sentencing.

Dated: July 19, 2011

Respectfully submitted,

ANDRÉ BIROTTE JR.
United States Attorney

ROBERT E. DUGDALE
Assistant United States Attorney
Chief, Criminal Division

/s/
STEPHANIE S. CHRISTENSEN
JENNIFER L. WILLIAMS
Assistant United States Attorneys

Attorneys for Plaintiff
UNITED STATES OF AMERICA

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

FEDERAL CASES: **PAGE(S)**

FEDERAL STATUTES:

TABLE OF AUTHORITIES (Continued)

FEDERAL STATUES: **PAGE(S)**

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Defendant Luis Mijangos is a 32-year-old, paraplegic, computer hacker who infected the computers of hundreds of victims by sending trojan emails and instant messages ("IMs") embedded with malicious software that gave him complete access to and control over the victims' computers. Defendant repeatedly committed such acts for over a year and a half. Defendant used this access to steal victims' financial information, which he sometimes passed along to a co-conspirator in Mexico.

Defendant did more than steal financial information through his hacking, however. He read victims' emails and IMs, watched them through their webcams, and listened to them through the microphones on their computers. Often, he then used the information he obtained to play psychological games with his victims. For example, he used intimate images or videos of female victims he stole or captured to "sextort" those victims, threatening to post those images/videos on the Internet unless the victims provided more to defendant; in at least one instance he followed through on his threat and publicly posted nude photos of a victim. He also tricked victims into creating pornographic images/videos by assuming the online identity of victims' boyfriends. Dozens of the victims are minors. Some of his victims thoroughly feared him and continued to be traumatized by his criminal conduct.

For his crimes, defendant was charged in a sixteen-count indictment filed on July 8, 2010, with charges including conspiracy, mail fraud, aggravated identity theft, possessing 15

or more unauthorized access devices, accessing a protected computer to obtain information (hacking), extortion, and wiretapping. He pleaded guilty on March 21, 2011, to two felony counts -- computer hacking and wiretapping -- pursuant to a written plea agreement.

On July 5, 2011, the United States Probation Office issued its Presentence Investigation Report ("PSR") in this matter. The total adjusted offense level as set forth in the PSR is 16, with a criminal history category of I, for a guidelines range of 21 to 27 months' imprisonment, in Zone D. The probation officer recommended 24 months' imprisonment followed by a three-year period of supervised release.

The government agrees with the PSR's criminal history calculation and offense level calculation with the following exceptions: sophisticated means (+2), use of special skills (+2), and 10+ victims (+2) enhancements should apply in this case, which together increase defendant's total offense level by an additional six points to a level 22. The government also objects to the absence of an upward departure, which is contemplated by the Guidelines for crimes like defendant's.

Based upon the factors set forth in 18 U.S.C. § 3553(a), including the deplorable nature of defendant's current crimes, the number and vulnerability of many of his victims, and defendant's sextortionate conduct, the government recommends that defendant be incarcerated for 84 months, to be followed by a three-year term of supervised release.

//

II. OBJECTIONS TO THE PSR

A. DEFENDANT DESERVES A SOPHISTICATED-MEANS ENHANCEMENT

USSG § 2B1.1(b)(9)(C) states: "if . . . the offense otherwise involved sophisticated means, increase by 2 levels." The commentary explains that "sophisticated means" include

> especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense. For example, in a telemarketing scheme, locating the main office of the scheme in one jurisdiction but locating soliciting operations in another jurisdiction ordinarily indicates sophisticated means. Conduct such as hiding assets or transactions, or both, through the use of fictitious entities, corporate shells, or offshore financial accounts also ordinarily indicates sophisticated means.

USSG § 2B1.1(b)(9)(C), cmt. n.8(B).

Here, defendant's crimes were "especially complex" and "especially intricate" in both the "execution" and "concealment" of the offense. Defendant most often electronically delivered the malicious software through an email or instant message. (See, e.g., PSR ¶¶ 15, 19, 20, 21, 25, 33). Defendant also admitted to planting malware on peer-to-peer networks disguised as song to lure unsuspecting victims. (PSR ¶ 33.) Often, having obtained the target's email address or IM user name from the infected computer of a friend of the target, defendant would usurp the identity of that infected friend and send the target the malware disguised as a video. (PSR ¶ 33.) Defendant used at least 30 different screen names to avoid detection. (PSR ¶ 25.) After he infected a victim's computer, defendant combed through the computer to obtain information he could further use to conceal himself (and infect/hack others). For example, in one instance, having learned from the victim's emails and computer

files that her ex-boyfriend had a conviction for stalking her, defendant contacted the victim pretending to have been hired by that stalker ex-boyfriend. (Ex. J at Bates 227).[1] His use of the malware also allowed him to watch victims through their webcams or listen to them through their computer microphones completely undetected, the ultimate in concealment. (PSR ¶¶ 18, 20, 22, 25; Ex. K.)

Defendant's use of the malware itself was also sophisticated and designed to conceal. Defendant used at least two types of malicious software, Poison Ivy and SpyNet, to gain remote access to victims' computers. (PSR ¶ 23; Ex. A at Bates 4147 (excerpt from draft transcript of defendant's statement to FBI during which he admits to using Remote Access Programs, such as Poison Ivy).) He also often used a "crypter," a hacking program or application used to hide viruses from antivirus programs so that they are not detected and deleted. (PSR ¶ 33.) Defendant also set up a separate website/host through which he routed the stolen data obtained from victims' computers and thereby further distanced himself from the crime. (PSR ¶ 24; Ex. A at Bates 4147 (defendant admitting that he used this remote host), Ex. B at 310, 315 (reports run on infected computer showing the remote host as "mijangos.no-ip.org"); Ex. C Compl. Aff. ¶ 9(b)(iii) (explaining that the remote host allowed defendant to control the infected computers through whatever computer he assigned to the host/domain).)

Although recognizing that defendant's use of the separate

[1] Exhibits G-O are filed under seal concurrently herewith.

webhost "indicate[d] some level of sophisticated means," the PSR failed to include the enhancement, reasoning that "the use of malware does not appear to be indicative of sophisticated means" and further that the enhancement should be determined "by reference to the typical means of committing the type of crime of which he is convicted." (PSR ¶ 50.) This was error.

As indicative above, defendant did much more than simply use malware, he went to great lengths in both the execution and concealment of his offense. He kept detailed files on many of his victims, filled with information he could later use to manipulate them. In some cases, he gathered these files for more than a month before contacting the victim. (See, e.g., PSR ¶ 15.)

Furthermore, the level of sophistication should not be viewed simply in terms of the hacking itself, but also in terms of the underlying crime. One of defendant's crimes of conviction was count 9, which charged defendant with hacking juvenile victim M.L.T.'s computer in furtherance of the another criminal act, specifically, violations of California Penal Code Section 647(j)(2) and (3), which criminalize the following:

> (2) Any person who uses a concealed camcorder, motion picture camera, or photographic camera of any type, to secretly videotape, film, photograph, or record by electronic means, another, identifiable person under or through the clothing being worn by that other person, for the purpose of viewing the body of, or the undergarments worn by, that other person, without the consent or knowledge of that other person, with the intent to arouse, appeal to, or gratify the lust, passions, or sexual desires of that person and invade the privacy of that other person, under circumstances in which the other person has a reasonable expectation of privacy.
>
> (3)(A) Any person who uses a concealed camcorder,

> motion picture camera, or photographic camera of any type, to secretly videotape, film, photograph, or record by electronic means, another, identifiable person who may be in a state of full or partial undress, for the purpose of viewing the body of, or the undergarments worn by, that other person, without the consent or knowledge of that other person, in the interior of a bedroom, bathroom, changing room, fitting room, dressing room, or tanning booth, or the interior of any other area in which that other person has a reasonable expectation of privacy, with the intent to invade the privacy of that other person.

This is not a case where defendant simply set up a camera in a dressing room, or even removed the peephole to take nude photographs of victims inside of hotel rooms as discussed in section III.C. below. As set forth in detail below, he took on the identity of a friend of the victim, tricked the victim into installing a malicious computer program on her computer (likely equipped with a special crypter that he often used to avoid antivirus detection), and then remotely stalked her capturing naked, intimate images of his unknowing, vulnerable, teenage victim.

At least one court has agreed that using a victim's own webcam to capture nude images of the victim constituted use of sophisticated means. See United States v. Feigin, 2010 WL 376278, at **1 (11th Cir. 2010) (per curiam) (unpublished) (district court imposed enhancements, unchallenged on appeal, for sophisticated means and use of special skill for hacker charged with violation of 18 U.S.C. § 1030(a)(2) who installed software on victim's computer, which software allowed him to use victim's webcam to capture nude photographs of victim); cf. United States v. Dinh, 2011 WL 1197666, at *3-*4 (S.D.N.Y. 2011) (applying sophisticated means enhancement for defendant convicted of

violation of 18 U.S.C. § 1030, who accessed currency company's computer system using Administrator logs and transferred currency).

Defendant's crimes are more complex than the average unauthorized access to a protected computer case. Given both the intricacy and the level of concealment of defendant's crimes, he qualifies for the sophisticated means enhancement.

B. DEFENDANT USED SPECIAL SKILLS TO COMMIT HIS CRIMES

USSG § 3B1.3 states: "If the defendant abused a position of public or private trust, or used a special skill, in a manner that significantly facilitated the commission or concealment of the offense, increase by 2 levels. . . ." Application note 4 explains that "'Special skill' refers to a skill not possessed by members of the general public and usually requiring substantial education, training or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts."

The Ninth Circuit has two requirements to apply the enhancement for use of a special skill: 1) defendant must use a skill not possessed by the general public, and 2) the skill must usually require substantial education, training or licensing. See United States v. Lee, 296 F.3d 792, 798 (9th Cir. 2002). A defendant, however, need not have acquired extensive education or training to qualify for this enhancement; it is enough that it is the type of skill usually requiring such training. See United States v. Peterson, 98 F.3d 502, 507 (9th Cir. 1996) (upholding enhancement for self-taught computer hacker and noting that "education, training, or licensing is not an absolute prerequisite for a special skill adjustment").

It is not enough that a defendant used a computer in committing his crime, he must possess and use computer skills, such as hacking to be worthy of the enhancement. Thus, the enhancement did not apply to a fraud defendant who simply replicated a legitimate website and captured credit card numbers of unsuspecting users who voluntarily went to the fake website. See Lee, 296 F.3d at 799 (noting that the enhancement applies only where a defendant's computer skills are particularly sophisticated). However, the enhancement did apply to a defendant who -- like the defendant here -- hacked computers and was convicted of computer crimes (18 U.S.C. § 1030) and wire tapping (18 U.S.C. § 2511). See Peterson, 98 F.3d at 504-05. In Peterson, the defendant worked with others to hack into the computers of financial companies to obtain credit card information and to wire money to himself, and hacked into phone company computers to seize telephone lines used to rig radio contests. Id. The use of these computer programming and hacking skills called for the enhancement. Id.

The denying the enhancement, the PSR stated that defendant and his conduct, was similar to the defendant's conduct in Lee where no enhancement was found. (PSR ¶ 55 & n.14.) This was incorrect. Lee merely copied an existing marathon registration website -- a task the court found did not even require much knowledge of the structure of the existing website -- and then collected the registration fees from registrants who were unaware they were visiting a fake website. 296 F.3d at 793-94. It was a basic fraud scheme that merely used the computer as tool.

Defendant Mijangos is much more similar to the defendant in Peterson. Like the defendant in Peterson, here defendant was convicted of a computer crime and wiretapping for hacking into protected computers. In committing his crimes, defendant used skills that are far beyond those possessed by the general public and usually require substantial education, training or licensing. In fact, defendant had specialized training in computer programming, having taken courses from Orange College in Costa Mesa, California. (PSR ¶¶ 32, 55.) Defendant programs in multiple computer programming languages (PSR ¶ 32; Ex. A at Bates 4156), and makes money as a computer programmer (PSR ¶ 13; Ex. A at Bates 4156.) In his own words, he takes orders from people who "know[] nothing about computers" and creates programs for them. (Ex. A at Bates 4170.) In addition to his formal computer training, like the defendant in Peterson, defendant learned much through cooperation with other hackers, and through networking on hacker websites such as Hackers.com and CC Power. (PSR ¶ 32; Ex. A at Bates 4225.)

Defendant used these special computer programming and hacking skills in committing his crimes. Defendant admitted that some of the programs he used were created for legal use and he adapts them for illegal activities. (Ex. A at Bates 4162.) He considered himself a "programmer" and a "hacker" and admitted to using the Internet to share information with others like him. (PSR ¶¶ 23, 32; Ex. A at Bates 4146, 4160-61.) As discussed above, defendant used multiple types of malware and he altered the malware to avoid anti-virus detection by using/creating crypters (PSR ¶ 33; Ex. A at Bates 4161-62) and set the program

to enable it to avoid forensic detection by exiting and closing down when it detected a forensic program. As discussed above, he also used a remote host rather than having the hacked information dump directly into his computer. Defendant also admitted to working with others outside the U.S. in complicated financial hacks that would earn him around $3,000/day. (PSR ¶ 22; Ex. A at Bates 4208-09.)

Defendant had both formal and informal training in computer programing and remote accessing, and he used those special skills to commit his computer hacking crimes. Therefore, the enhancement should apply. See United States v. Feigin, 2010 WL 376278, at **1 (11th Cir. 2010) (per curiam) (unpublished) (district court imposed enhancements, unchallenged on appeal, for sophisticated means and use of special skill for hacker charged with violation of 18 U.S.C. § 1030(a)(2) who installed software on victim's computer which software allowed him to use victim's webcam to capture nude photographs of victim).

C. DEFENDANT DESERVES AN ENHANCEMENT FOR THE NUMBER OF VICTIMS

Under USSG § 2B1.1(b)(2)(A), a two-level enhancement is applied if the offense "involved 10 or more victims." Effective November 1, 2009, "victim" includes "any individual whose means of identification was used unlawfully or without authority," regardless of whether the individual sustained an actual monetary loss (a former prerequisite for victim classification under this section). USSG § 2B1.1, cmt. n.4(E). "'Means of identification' has the meaning given that term in 18 U.S.C. § 1028(d)(7)." USSG § 2B1.1 cmt. n.1. Under § 1028(d)(7), "means of identification" includes "any name or number that may be used, alone or in

conjunction with any other information, to identify a specific individual, including any . . . name . . . or electronic identification number [or] address."

Here, since November 1, 2009, defendant used the unique instant messenger screen names -- which are both names and electronic addresses under the plain language of § 1028(d)(7) -- of at least 31 different victims.[2] (PSR ¶ 47.) Indeed, defendant used these victims' screen names in order to assume fully the victims' online identities, connect with their friends and family (who believed they were chatting with the real victims, when it fact it was the defendant), and pass along links that, once clicked, would infect the new victim computer with malware. (PSR ¶ 25.) Accordingly, a two-level enhancement under USSG § 2B1.1(b)(2)(A) applies. Cf. United States v. Yummi, 2010 WL 4872210, at *2 (3d Cir. Nov. 17, 2010) (unpublished) (district court properly applied two-level victim enhancement where defendant either sent or received emails that included personal information, such as names, addresses, and birth dates identifying more than ten victims); United States v. Craig, 343 F. App'x 766, 769 (3d Cir. 2009) (e-Bay account is a "means of identification") (unpublished); United States v. Geeslin, 236 F. App'x 885 (5th Cir. 2007) (personal telephone number qualified as

[2] To be sure, as set forth throughout, defendant used the identities of well over 31 victims to infect new victims' computers. Because the guideline amendment including as victims those who did not incur an actual monetary loss did not take effect until November 1, 2009, only those victims whose identities were used by defendant after that date have been counted for the purpose of the two-level enhancement. All victims are, of course, considered in the evaluation of the § 3553(a) factors set forth below.

"means of identification") (unpublished).

The PSR denied this enhancement, noting that no Ninth Circuit case law has yet addressed the issue. (PSR ¶ 46.) The PSR stated that the Sentencing Commission expanded the definition of "victim" to account for the lost time often experienced by those individuals in resolving credit problems and related issues, despite the fact that they may not have suffered an actual loss. (PSR ¶ 46, citing Appendix C, Amendment 726, to the United States Sentencing Commission Manual, November 1, 2009, hereinafter "Amendment 726").) This reading is too narrow and conflicts with the plain language and legislative history of the guideline, which counts as victims those whose means of identification were used unlawfully.

First, under the plain language of the amendment, a screen name, which is a unique name/address associated with an individual for the purpose of sending IMs (which essentially are instant emails, in which links can be included), qualifies as a means of identification because it is both a "name" and an "electronic address" that permits the sending of messages. Defendant "used" these "means of identification" when he sent and received IMs to/from new victims. Although there is no Ninth Circuit case on point, the unpublished case cited above serve as guidance, finding both online accounts and personal telephone numbers to be "means of identification" (as they "identify a specific individual"), Craig, 343 F. App'x at 769; Geeslin, 236 F. App'x at 885, and that emailing "means of identification" is an unlawful use, Yummi, 2010 WL 4872210, at **2.

Second, the legislative history of the guideline amendment

supports application in this case. As noted in Amendment 726, the November 1, 2009 amendment responded to a Congressional directive in section 209 of the Identity Theft Enforcement and Restitution Act of 2008, Title II of Publ. L. 110-326 (the "Act"). The Act directed the Sentencing Commission to consider, and account for, thirteen listed factors, in order to reflect the intent of Congress that penalties be increased and to "create an effective deterrent to computer crime and the theft or misuse of personally identifiable data." See Amendment 726 at section "Reason for Amendment" and the Act at § 209(a) & (b). Included in such factors -- to be accounted for by the Commission -- was "[w]hether the term "victim" . . . should include individuals whose privacy was violated as a result of the offense in addition to individuals who suffered monetary harm as a result of the offense." See the Act at 209(b)(12) (emphasis added). Accordingly the reading of "victim" in the PSR is too narrow: although the new, broader, definition accounts for victims who lost time in resolving credit problems (despite not sustaining monetary loss), in also includes victims whose privacy was violated because a means of their identification was used unlawfully.

The 31 individuals in this case whose online identities were stolen, so that the defendant could send infectious links to their friends and family, were victims under the guidelines. The enhancement should be applied.

D. DEFENDANT DESERVES AN UPWARD DEPARTURE

USSG § 2B1.1 is the Guidelines section used for section 1030 offenses like that to which defendant pleaded guilty. This is

the same section used for offenses involving, among other things, theft, stolen property, property damage or destruction, fraud, forgery, and counterfeiting, and generally gauges the seriousness of the offense by the amount of monetary loss. The commentary recognizes, however, that an upward departure is warranted where the nature of the crime is non-monetary. See USSG § 2B1.1 cmt. n.19. Among the non-exhaustive list of factors warranting an upward departure are the following:

> (i) A primary objective of the offense was an aggravating, non-monetary objective. For example, a primary objective was to inflict emotional harm.
>
> (ii) The offense caused or risked substantial non-monetary harm. For example, the offense cause physical harm, psychological harm, or severe emotional trauma, or resulted in substantial invasion of a privacy interest (through, for example, the theft of personal information such as medical, educational, or financial records). . . .

The PSR noted this upward departure language, but made no determination regarding its applicability. (PSR ¶ 141.) A substantial upward departure is warranted for this defendant because the monetary adjustments in § 2B1.1 do not properly capture the seriousness of defendant's conduct.

In his interview by law enforcement, defendant admitted that he worked with "black hat" hackers, made money transfers for the group, and conducted other financial scams with them. (PSR ¶ 32; Ex. A at Bates 4160, 4168, 4203.) However, defendant was motivated in large part by non-monetary objectives. He could have hacked into victim computers, obtained financial information, deleted the malware, and left undetected. Instead, he made contact with his victims and played psychological games with them intending to inflict emotional harm. In fact, many of

the section 1030 predicates charged in the indictment were tortious actions for intentional infliction of emotional distress, e.g., counts 4-8, 11. He also "sextorted" and threatened his victims. (PSR ¶¶ 15, 16, 19; Ex. A at Bates 4192, 4209 (defendant admitting that he threatened victims to prevent them from contacting the police and asked them to produce additional sexual videos).) Defendant admitted to "fucking around with his victims" by contacting them. (PSR ¶ 34; Ex. A at Bates 4183.)

Additionally, through his hacking, defendant amassed a collection of child pornography, i.e., photographs/digitally captured images of minors engaged in sexually explicit conduct. (PSR ¶ 20; Ex. D (FBI table detailing all the locations defendant had child pornography (CP), malware (Mal) and identity theft materials (ID).) Possession of child pornography itself is a very serious crime. See 18 U.S.C. § 2252A; USSG § 2G2.2. The § 2B1.1 adjustments do not account for this.

Although defendant had hundreds of victims, dozens of whom were juveniles (PSR ¶ 22), some particularly distributing examples of his conduct relating to intentional infliction of emotional distress and collection of child pornography are below.

1. Victims D.D. and A.V.

Defendant dedicated considerable time to toying with victims D.D. (counts 4, 5, and 13) and A.V. (count 4). (PSR ¶ 15.) D.D. and A.V. were formerly dating and defendant infected both of their computers. (PSR ¶ 15.) Defendant IM'd A.V. asking her to have web sex, claiming to know her, and reporting intimate details about her including a description of her bedroom. (Id.)

Defendant sent A.V. naked photos of A.V., obtained from D.D.'s computer. (Id.) When A.V. IM'd D.D. about defendant's conduct, defendant knew, having infected their computers, and then sent threats to both of them. (Id.) He was also able to intercept their oral communications and pleaded guilty to wiretapping D.D. (Id.; and count 13.) A.V. contacted campus police to report defendant, and while officers were in her room taking a statement, defendant listened through the microphone of her roommate's computer, which he had also infected, and then sent more threatening emails to D.D. because A.V. had contacted the police. (PSR ¶ 15.) A file with keylogger information obtained from A.V.'s computer as well as images of D.D. and A.V. having web sex were recovered during a search of defendant's computer. (Id.)

When later interviewed by the FBI, A.V. "was visibly upset and shaking during parts of the interview and had to stop at points to control her emotions and stop herself from crying." (Ex. G at Bates 94.) She reported feeling "terrorized" by defendant, was afraid for her safety, and did not leave her dorm room for a week after the episode. (Id.; PSR ¶ 29.) D.D. submitted a victim impact statement in which he relayed the mixture of anger, fear, anxiety, and confusion caused by defendant. (Ex. H.) He also reported trouble concentrating, appetite change, increased school and family stress, lack of trust in others, and a desire to be alone. (Id.) The stress of the crime was too much for D.D. and A.V. and it led to the end of their relationship. (Id.; PSR ¶ 28.) The impact went beyond D.D. to his family, as he reported that his parents "had a hard

time trusting anyone or even feeling comfortable enough to use a computer." (Id.)

2. Victim S.G.

Victim S.G. (count 6) was a juvenile when defendant hacked into her computer and sextorted her. (PSR ¶ 76.)[3] Using a screen name similar to that of S.G.'s then-boyfriend, defendant IM'd her and asked her to send him pornographic photos, and she complied. (PSR ¶ 76.) When she discovered it was not her boyfriend, defendant changed screen names and later "sextorted" S.G. telling her he would post the nude photos of her online if she refused to send him more. (Id.) Seeking help, S.G. emailed copies of defendant's threats to her boyfriend. (Id.) Having complete access to S.G.'s computer, defendant tracked these communications and confronted S.G. (Id.) Defendant even went so far as to obtain S.G.'s phone number and called her. (Id.) A keylogger file capturing defendant's IM conversation where he sextorts young S.G. was recovered from defendant's computer. (Id.)

S.G. completed a victim impact statement which illustrates the psychological harm defendant's crimes had on his victims. S.G. reported having nightmares, trouble concentrating, appetite change, repeated memories of the crime, and a fear that defendant would return. (Ex. I.) Of defendant's conduct she wrote:

> It made me untrusting and paranoid to this day. For the longest time I didn't know who this man was, why he

[3] The PSR put details about victims S.G. and K.S. under the heading "Offense Behavior Not Part of Relevant Conduct." (PSR ¶¶ 74-76.) The government believes the computer hacks of these victims are part of the same course of conduct and should be included in relevant conduct.

> was doing it or [if] he would come back. Not knowing is the worst, most dreaded feeling. It's always in the back of your mind. I moved away from the LA/OC area but even here the thoughts never left me. . . . When I learned more girls had gone through the same thing I was so angry. . . . Never could I imagine what others felt.

(Id.)

3. Victim L.W.

Defendant's attack on victim L.W. (Count 7) involved threats to expose secrets obtained from her email to her family. (PSR ¶ 16.) From reading her personal documents/communications, defendant learned that L.W.'s father was a devout Jehovah's Witness. (PSR ¶ 16.) After finding nude photos of L.W. on her computer, defendant sent her an email titled "you had a tasty pussy" and later in the exchange wrote: "I wonder what you dad would say if I show this pic, a jehova believer umm umm ummm" (sic). (Id.) Defendant also threatened to post the nude photos on MySpace and Facebook if she did not make a deal with him. (Id.) A search of defendant's computer revealed hundreds of pages of transactions from L.W.'s computer. (Id.) Defendant had also burned nude photos of L.W. to a separate CD. (Id.)

4. Victims G.M. and E.M.

Defendant posted nude photos of victim G.M. (count 8) on the Internet after she refused defendant's sextortionate demands. (PSR ¶ 19.) After hacking her computer, defendant contacted G.M. by email with the subject line "who hacked your account READ it!!!" wherein he pretended that G.M.'s ex-boyfriend had hired him to hack her account. (Id.) This was particularly traumatic for G.M. because she had a restraining order against the ex-boyfriend, who was on probation for harassing her. (Ex. J at

Bates 227.) Defendant told G.M. to be "smart" and "cool" and claimed he would help her. (Id. at Bates 226-32.) When G.M. did not immediately respond, defendant sent another email attaching a nude photo of G.M. and stating "im going to post those all over, facebook, myspace. here's the pic." (Id.) Defendant claimed to be a part of "a team of hackers." (Id.) When defendant discovered, by monitoring her computer, that G.M. had sent her friend -- victim E.M. -- copies of defendant's threatening communications, defendant sent an email saying "you pissed me off now I'm going to show you." (Id.) He then posted nude photos of G.M. on E.M.'s MySpace page, which page defendant had hacked into, having also infected E.M.'s computer. (Id.; Ex. K.) Several pornographic photos of G.M. were found on defendant's computer at the time of the search including the one he used to sextort her. (Id.)

When interviewed by the FBI, G.M. reported that she felt as if her life had been taken away. (PSR ¶ 30; Ex. J at Bates 225.) She further relayed that she no longer felt safe having any personal information on her computer. (Id.)

5. Victim C.G.

Defendant sent victim C.G. (count 5) an email with a naked photo of her and the message "nice video I hope you still remember this if you want to chat and find out before I put it online hit me up." (PSR ¶ 17.) On his computer defendant had photos of C.G. having web sex with victim D.D., other photos of her, and her IM screen name. (Id.)

6. Victim M.L.T

Defendant pleaded guilty to count 9 concerning victim M.L.T.

She was a juvenile still in highschool when defendant hacked her computer, through the hacked computer of M.L.T's friend. (PSR ¶ 20; Ex. L at Bates 11.) By watching M.L.T. in real time while she was having web sex with her teenage boyfriend, defendant captured and saved to his computer some nearly 3,000 images. (Id.) Defendant would turn her webcam on and off periodically watching M.L.T. (Id.) Defendant also stole financial information of M.L.T.'s parents victimizing the entire family. (Id.; Ex. L at Bates 7, Ex. M.)

7. Victim A.M.

Victim A.M. (count 11) was also in highschool when defendant hacked into her computer. (PSR ¶ 21.) Defendant assumed the IM name of one of her friends (another hacking victim) and IM'd her a link containing the malicious software that enabled him to hack her computer. (Id.) Pretending to be the friend, defendant asked A.M. to have "cybersex;" she refused and then discovered that it was not her friend IM'ing her. (Id.) Defendant later used a different screen name to IM A.M.: "hey would you do masturbation videos for money?" (Id.) Hundreds of pages of keylogger files and photos of A.M. were recovered from defendant's computer. (Id.)

8. Victim S.S.

Defendant would listen and record victim S.S. (count 14) using the microphone on her hacked computer. (PSR ¶ 18.) An audio file of S.S. talking on her phone was recovered from defendant's computer along with log files including a paper she wrote as part of her schoolwork. (PSR ¶ 18.)

9. Victim K.S.

Defendant also "sextorted" victim K.S. and even included details about her children and work in his threats. (PSR ¶ 74; Ex. N at Bates 50.) Defendant hacked into K.S.'s computer and obtained nude photos of her from her email account. (Ex. N at Bates 49.) He also obtained personal information about her job (as an escort) and family. (Ex. N at Bates 50.) Defendant emailed K.S. nude photos of herself titled "read this and be smart" with threatening text discussing her children, her work (using HumaniPlex), and her ex-boyfriend. (PSR ¶ 74; Ex. N at Bates 50.) In the body, defendant demands that she send him "a porn video" and threatens that is she refuses he will publish the photos and "let your family know about your dark side as a hooker." (Id.) In his interview with law enforcement, defendant admitted to targeting users of a website called "HumaniPlex," which is a social networking site frequently used by escorts. (Ex. A at Bates 4181.) Defendant targeted users of HumaniPlex, like K.S., knowing that it would be easy to trick them into clicking on malware links due to the volume of email they received. (Ex. A at Bates 4181.)

The above is merely a sampling of the emotional trauma and psychological harm defendant inflicted on his victims. Absent the upward departure, the Guidelines do not capture this conduct. Nor do they capture the severe invasions of privacy perpetrated by defendant. As noted in the PSR numerous videos appearing to be from unauthorized activation of webcams were discovered on defendant's computer, which included victims getting out of the shower, dressing, and having sex. Many of the subjects were

unidentified. (PSR ¶ 22 n.4.)

III. THE APPROPRIATE SENTENCE UNDER THE 3553(A) FACTORS

Taking the advisory Guidelines into consideration, including the upward departure, the government believes that a sentence including 84 months' imprisonment is sufficient but not greater than necessary to comply with the enumerated purposes of sentencing and the factors set forth in 18 U.S.C. § 3553(a).

A. 18 U.S.C. § 3553(a)(1)

18 U.S.C. § 3553(a)(1) requires the Court to consider the nature and circumstances of the offense and the history and characteristics of defendant. Defendant's crimes and the impact on his victims were truly terrible. The emotional distress caused to the victims is a necessary part of the evaluation of the nature and circumstances of defendant's offense. See, e.g., United States v. Moon, 513 F.3d 527, 534 (6th Cir. 2008) (affirming sentence where district court permitted testimony of relatives of deceased patients as relevant to nature and circumstances of the fraud offense).[4]

Moreover, as detailed in the PSR and above, defendant's conduct spanned well over a year, involved financial, wiretapping, and computer hacking crimes, and victimized hundreds of people, including dozens of juveniles. (PSR ¶ 22.) The number of victims is not captured by the Guidelines' artificially

---

[4] Some courts have considered harm to the victim under Section 3553(a)(2) as well. See, e.g., United States v. Gonzalez, 541 F.3d 1250, 1254 (11th Cir. 2008) (noting district court's consideration of "desperation of the victims" when considering the nature and circumstances of offense and harm to victims when considering the need to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment).

narrow definition of "victim" and should be considered under the 3553(a) factors. See USSG § 2B1.1 app. n.1.

As to defendant's history and characteristics, he is a 32-year old man who is unable to walk due to a gunshot wound inflicted approximately 15 years ago when he was a teenager. (PSR ¶ 98.) He reported a difficult childhood in Mexico resulting from the harassment and death of his father, but his mother remarried in the U.S. and he has had a stable family environment for more than 15 years. (PSR ¶¶ 93-96.) As an adult, defendant worked to acquire significant computer skills. He studied computer science at a local college, gaining knowledge of various programming languages. (PSR ¶ 32.) For several years he worked as a freelance computer technician and programmer, including as a website developer. (PSR ¶¶ 13, 32.) He reported to agents that he earned, on average, $1,000 per week. (Compl. Aff. ¶ 7a (attached as Ex. C).) However, despite his family support and ability to contribute to society, defendant chose to use his skills to break the law and victimize others.

B. 18 U.S.C. § 3553(a)(2)

18 U.S.C. § 3553(a)(2) requires the Court to consider the need for the sentence to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of defendant, and to provide defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner. This factor also supports the government's recommended sentence.

A significant period of incarceration is necessary given the serious nature of defendant's offense, including the number of victims and the depth of harm he inflicted on them. In the opinion of one victim "anything less than 10 [years] is insulting." (Ex. I at 2.)

A lengthy sentence is also necessary to promote respect for the law and for specific deterrence. In March 2010, the FBI executed a search warrant at defendant's residence, during which time defendant gave a partial confession minimizing his conduct. (Ex. C, Compl. Aff. ¶¶ 6-7.) After execution of the warrant and knowledge that his hacking activities were being investigated, defendant continued to commit crimes and victimize others. As the affidavit in support of the complaint explains, several victims reported activity after the time of the search warrant and defendant continued to use his domain "mijangos.no-ip.org" after the search. (Ex. C, Compl. Aff. ¶¶ 10-17.) In addition, defendant's punishment should be severe enough not only to serve as a deterrent for him, but also to other hackers who contemplate such activities.

Finally, incarceration will also result in adequate medical care for defendant. Based on a review of defendant's medical records, the Associate Warden and FCI Terminal Island prepared a lengthy declaration explaining that the Bureau of Prisons (BOP) can accommodate defendant's conditions. (Ex. O.) In it, he explains that BOP manages the health of numerous inmates with medical needs similar to defendant's and that there at least eight individuals with similar conditions at his institution alone. (Ex. O at ¶ 6.) He explained in detail the monitoring

provided by BOP for inmates with defendant's conditions (¶¶ 15-17) and the urgent care available, explaining that, in his experience, "rather than resulting in delay in the delivery of emergency care, the correctional setting is one that lends itself to quick response time" (¶ 18). He further explained that all of defendant's medications can be provided for (¶ 20) and that defendant's mental health issues "are ones that the BOP is equipped to handle" (¶ 22). Accordingly, correctional treatment can be provided in an effective manner even taking into account defendant's chronic condition.

C. 18 U.S.C. § 3553(a)(6)

18 U.S.C. § 3553(a)(6) requires the Court to minimize sentencing disparity among similarly situated defendants. This factor is extremely important. While normally a Guidelines sentence helps to prevent sentencing disparities, here it would create one. As explained above, the applicable Guidelines simply do not capture the seriousness and depth of defendant's conduct, particularly with regard to defendant's watching and listening to victims through their webcams and capturing intimate, nude images of them.

United States v. Feigin, involved similar conduct by a defendant convicted of a violation of 18 U.S.C. § 1030, for installing malware on the computer of an adult, female victim, which allowed him to capture nude images of the victim through her webcam. 2010 WL 376278, at **1 (11th Cir. 2010) (per curiam) (unpublished). As in this case, the victim reported a lasting impact from the crime, including insomnia, paranoia, anxiety, and issues with trust and insecurity. Id. The district court

imposed a sentence nearly two times greater than the high end of the advisory Guidelines range. Id. at **6. This 30 month-sentence was upheld by the Eleventh Circuit in an unpublished opinion which recognized that the financial focus of USSG § 2B1.1 failed to capture the deliberate invasion of privacy and lasting the harm to the victim. Id. at **7-8. Notably, defendant's conduct in the instant matter is significantly worse, as it involved hundreds of victims (not just one), many juveniles (as opposed to the single adult), and sextortion and threats to the victims (absent in Feigin).

In a case from this district, last summer, defendant Michael David Barrett was sentenced to 30 months' imprisonment for capturing nude images of ESPN reporter Erin Andrews. (Ex. E.) Defendant captured the images by removing the peepholes from the victim's hotel room doors and snapping pictures inside the rooms. (Ex. F at 1.) The defendant was convicted of stalking, 18 U.S.C. § 2261A(2)(A). (Ex. E.) The conduct in the two cases is similar in that both involved defendants who surreptitiously captured nude images of victims. An even lengthier sentence is called for in the instant matter, however, due to the hundreds of victims, the intimate/sexual nature of many of the images captured, the vulnerability/age of many of the victims, and defendant's sextortionate demands.

D. THE REMAINING 3553(A) FACTORS ALSO SUPPORT THE SENTENCE REQUESTED BY THE GOVERNMENT

18 U.S.C. § 3553(a)(3) requires the Court to consider the kinds of sentences available. Incarceration is appropriate given the serious nature of defendant's offense and his role. 18

U.S.C. § 3553(a)(4) & (5) now merely require the Court to take the sentencing Guidelines as "advisory."

18 U.S.C. § 3553(a)(7) requires the Court to consider restitution. Under the Mandatory Victims Restitution Act ("MVRA"), restitution is mandatory where "an identifiable victim or victims has suffered . . . pecuniary loss." 18 U.S.C. § 3663A(c)(1)(B). The restitution amount to date is $1,964.46 owed to victim S.M. for fraudulent charges made to his Union Bank account. (PSR ¶ 23.)[5] Other victims reported expenses including computer repair (for removal of the malware) and the purchase of new computers but documentation could not be provided (PSR ¶ 27) and thus those sums are not included in the restitution amount.

IV. CONCLUSION

For all the foregoing reasons, the government requests that the Court impose a sentence of 84 months' imprisonment, a three-year period of supervised release, restitution in the amount of $1,964.46, and a special assessment of $200.

Dated: July 19, 2011

Respectfully submitted,

ANDRÉ BIROTTE JR.
United States Attorney

ROBERT E. DUGDALE
Assistant United States Attorney
Chief, Criminal Division

/s/
STEPHANIE S. CHRISTENSEN
JENNIFER L. WILLIAMS
Assistant United States Attorneys

Attorneys for Plaintiff
UNITED STATES OF AMERICA

[5] Although noting this monetary loss at paragraph 23 of the PSR, paragraph 140 confusingly states that restitution information was not provided.