UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
CENTRAL DIVISION
LEXINGTON

CRIMINAL ACTION NO. 5:16-CR-62-DCR

UNITED STATES OF AMERICA

V. **UNITED STATES' SENTENCING MEMORANDUM**

DERIC LOSTUTTER

* * * * *

Deric Lostutter pleaded guilty to conspiring to illegally access a computer and making false statements to federal agents (R. 72). As a condition of his plea agreement, Lostutter agreed that his offense involved sophisticated means and he intentionally engaged in and caused the conduct constituting sophisticated means (R. 72 at ¶ 6(c)). Lostutter now objects that his conduct did not involve sophisticated means. The United States requests that the Court impose imprisonment at the upper end of the range of 18-24 months calculated by the Probation Office, including the agreed-upon increase for sophisticated means.

The PSR properly increases Lostutter's offense level under U.S.S.G. § 2B1.1(b)(10) (PSR ¶ 29), because, as Lostutter agreed (R. 72 at ¶ 6(c)), the computer attack involved "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." § 2B1.1 cmt. n.9(B). In addition to admitting the multiple and coordinated steps required to execute the crime (R. 72 at ¶ 4(c-g)), Lostutter admitted using a virtual private networking service to anonymize Internet

activity (R. 72 at ¶ 4(c)), and redirecting the fan website to a different Internet host in a foreign country so that the administrator of the fan website could not regain control of the fan website (R. 72 at ¶ 4(h)). These actions are analogous to "hiding assets or transactions, or both, through the use of fictitious entities, corporate shells, or offshore financial accounts." § 2B1.1 cmt. n.9(B). This conduct demonstrates the use of sophisticated means not only to execute Lostutter's crime, but also to conceal it.

A sentence at the upper end of the guidelines range is appropriate "to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense." 18 U.S.C. § 3553(a)(2)(A). Until his release conditions were modified (R. 30), Lostutter promoted a false media narrative justifying his crime as necessary to solve the August 2012 rape of a high school student in Ohio, *see* Exhibit 1, ignoring that all the evidence was previously known and both rapists were arrested months before his December 2012 computer hack (PSR ¶ 5). Throughout his prosecution, Lostutter has collected money by posing as a whistleblower who stopped a media coverup and police corruption, *see* Exhibit 2, fraudulently concealing that the rape case received national press attention before his involvement (R. 72 at ¶ 4(a)) and that his threatening video intimidated the government's witnesses. During his explanation of the facts at his rearraignment proceeding (R. 70), Lostutter again justified his crime, falsely claiming that he needed to "do something about it because no one else did."

Lostutter's self-promotion and self-congratulation never acknowledge that his illegal actions defamed a fan website operator as a child pornographer and director of a

"rape crew," threatened to do the same to a list of high school students, and invaded the privacy of unconnected adult women by publicly posting their emails containing nude photographs (PSR ¶¶ 6, 12, 18). Nor does he give any logical reason why he thought it helped the rape victim to publicly post this defamatory manifesto, private emails, and threatening video (which included a picture of the rape victim). Nor does he explain why he reasonably believed that it was necessary, or even helpful, for him to punish and threaten strangers without due process, from behind a virtual private networking service and a Guy Fawkes mask. Lostutter's actual motive was to gain publicity for his online username (R. 72 at ¶ 4(c, i)), without regard for the real repercussions to real human beings. A sentence at the upper end of the guidelines range is necessary to finally reflect the seriousness of this offense.

If Lostutter's crime was helpful and necessary, he would not have lied to FBI agents about his role in the conspiracy (PSR ¶ 2). If Lostutter's interest was justice, he would not have given self-serving sworn testimony in this Court that was judged "inherently incredible," "fanciful," "utterly unbelievable," and "blatantly inaccurate" (R. 60 at 23-24). Lostutter's repeated obstructions show contempt for the justice system. An upper end of the guidelines range sentence is necessary to promote respect for the law.

A sentence at the upper end of the guidelines range is appropriate "to afford adequate deterrence to criminal conduct." § 3553(a)(2)(B). Here, this deterrence is not theoretical. After their hack, Lostutter's co-conspirator sent him messages joking that they would never be prosecuted or imprisoned for their computer crime. *See* Exhibit 3;

R. 72 at ¶ 4(i). Lostutter's sentence of imprisonment must ensure that other hackers understand that hacks will be taken seriously as crimes, not as pranks or publicity stunts. Some people will continue to use easily-guessed online passwords; that is not a license for others to hack and humiliate them from behind a computer screen without real-world consequences. Here, Lostutter identifies himself as "KYAnonymous," a member of a computer hacking organization called Anonymous (R. 72 at ¶ 4(a)). A sentence at the upper end of the guidelines range is necessary to deter his fellow hackers from exploiting other people's online vulnerabilities and invading their privacy; a low sentence may reinforce the opposite message.

Lostutter may not argue that any collateral consequences over the past few years are already sufficient deterrence (PSR ¶¶ 62-64). § 3553(a)(2)(B) requires "*the sentence* imposed . . . to afford adequate deterrence to criminal conduct" (emphasis added).

A guidelines sentence is appropriate "to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner." § 3553(a)(2)(D). The United States believes that Lostutter would benefit from participation in a federal prison's vocational training program.

Imprisonment at the upper end of the guidelines range of 18-24 months is appropriate "to protect the public from further crimes of the defendant." § 3553(a)(2)(C). After an itinerant career (PSR ¶¶ 67-68), Lostutter found fame as a computer hacker (PSR ¶ 71). Since then, he seemingly cannot stop harassing others online (PSR ¶¶ 3, 74-78), even opening an "investigation" business for online harassment on behalf of clients

(R. 30 at n.2). In the face of a specific Court order not to use the Internet to threaten or harass any other person (R. 18), Lostutter violated that release condition within days (R. 30, 64 at 2). Lostutter's self-promotion and justification of his computer crime, his false statements to the FBI and to this Court, and his continued online harassment of other victims make Lostutter's record unfavorably dissimilar to other defendants who have been found guilty of similar conduct.[1] § 3553(a)(6). The only appropriate way to end Lostutter's computer hacking career is to incapacitate him in prison for a sentence of imprisonment at the upper end of the guidelines range calculated by the Probation Office.

Respectfully submitted,

CARLTON S. SHIER, IV
ACTING UNITED STATES ATTORNEY

By: s/ Neeraj K. Gupta
Assistant United States Attorney
260 W. Vine Street, Suite 300
Lexington, Kentucky 40507-1612
(859) 685-4843
Neeraj.Gupta@usdoj.gov

CERTIFICATE OF SERVICE

On March 1, 2017, I electronically filed this document through the ECF system.

s/ Neeraj Gupta
Assistant United States Attorney

[1] Lostutter's sentencing memorandum incorrectly suggests computer hackers do not receive long prison sentences. *See, e.g.*, Brian Johnson received 34 months imprisonment in the Middle District of Louisiana in 2017 for hacking into an industrial facility; Chris Correa received 46 months imprisonment in the Southern District of Texas in 2016 for hacking into the Houston Astros; Ryan Collins received 18 months imprisonment in the Central District of California in 2016 for hacking into female celebrity email accounts; Matthew Keys received 24 months imprisonment in the Eastern District of California in 2016 for hacking into The Los Angeles Times; Anastasio Laoutaris received 115 months imprisonment in the Northern District of Texas in 2016 for hacking into a law firm.