BENJAMIN B. WAGNER
United States Attorney
MATTHEW D. SEGAL
PAUL HEMESATH
Assistant United States Attorneys
501 I Street, Suite 10-100
Sacramento, CA 95814
Telephone: (916) 554-2700
Facsimile: (916) 554-2900

LESLIE R. CALDWELL
Assistant Attorney General
United States Department of Justice, Criminal Division
JAMES SILVER
Deputy Chief for Litigation
Computer Crime and Intellectual Property Section
Washington, DC 20530
Telephone: (202) 514-1026

Attorneys for Plaintiff
United States of America

IN THE UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW KEYS, Defendant.	CASE NO. 2:13-CR-82 KJM SENTENCING MEMORANDUM OF THE UNITED STATES - *CORRECTED* DATE: March 23, 2016 TIME: 9:00 a.m. COURT: Hon. Kimberly J. Mueller

I. INTRODUCTION

The United States recommends that the Court impose a sentence of sixty months imprisonment. The Probation Department's recommendation of eighty-seven months is reasonable and the best way to promote sentencing uniformity. But this prosecutor has been with this case since its inception in 2010 and submits that a five-year sentence as sufficient, but not greater than necessary, to comply with the purposes of sentencing. A sentence of five years imprisonment reflects Keys's culpability and places his case appropriately among those of other white collar criminals who do not accept responsibility for their crimes.

II. FACTS

A. The Offense Conduct

Matthew Keys was the site administrator for Fox 40 on Tribune Company's content management system ("CMS"). Tribune terminated Keys's known CMS credentials on the day he was dismissed from the newsroom. But for two months after that, Keys remained bitter, angry, and in control of login credentials that he had secretly created while at the company. He also had his administrator's knowledge of the CMS's architecture and vulnerabilities.

At first, Keys used what skills and knowledge he had to steal the list of the email addresses of Fox 40's viewers who had signed up for an affinity program, and, in many cases, given over their credit card numbers. Through a proxy server, Keys sent anonymous, harassing emails to his former viewers and colleagues.

That Keys intended to harm Fox 40 is obvious. Keys confessed that he wanted for there to be consequences for his being hurt by Fox 40. (Dkt. 23-5 at 54.) He reveled in his power over Fox 40. As "Cancer Man," he bragged to Brandon Mercer, "you guys make it incredibly easy to gain access to your subscriber list," and, then, later, copied text about how easily a corporation's security technology could be undermined by "a determined insider" who decides to "go rogue." (GX 108, 109.) In an email to Fox 40's most interested viewers, he suggested that Fox 40 was "spying on you, turning your credit card statement into advertising GOLD[.]" (GX 107.)

Confident in his anonymity behind a foreign proxy server, (GX 103), Keys was also entirely willing to inflict substantial collateral harm in the offline world. On December 3, 2010, when told about the "crying senior citizen" who was worried about her account during her husband's kidney failure, Keys ridiculed Fox 40 for "report[ing] to the old folks home," and suggested that the woman's response indicated her "priorities [were] in the wrong place." (GX 1004.) Later the same day, Keys taunted Fox 40 with more stolen emails and asked, "think any of these guys are elderly?" (GX 108.)

On December 6, 2010, Keys sent an email to viewers excoriating a Fox 40 reporter for making a woman cry. (GX 111.) He also started an eight-day campaign of accessing the CMS to lock his replacement out of the CMS. (GX 112.) Keys knew what effect he was having. He later said, "I believe that Brandon [Mercer] was terrified." (Dkt. 23-5 at 56.)

Then Keys found Anonymous, whom he called "A group of individuals who could do significant damage . . . and not get[] caught." (Dkt. 23-5 at 33.) Keys called Anonymous "malicious without a cause," and "the people who were doing the most damage." (*Id.*) He was amazed by "the skill that was in that chat room and blatant disregard for any kind of consequence." (*Id.*) What did he do? On December 8, 2010, Keys created and gave Anonymous backdoor access to the Tribune Company CMS and told them what Tribune Company properties to target. (GX611.) Nothing obvious immediately happened, so he spent days repeatedly urging Anonymous to "demolish" a major American newspaper because of what it had published. On December 9, 2010, he posted a link to a *Los Angeles Times* piece critical of Wikileaks and wrote, "Yet another reason the Times must be demolished." (GX 607.) On December 10, 2010, when a member of Anonymous stated opposition to attacking media, Keys responded, "FOX News is not media, it's 'infotainment' for inbreds. I say we target them." (GX 608-609.)

Keys thus had good reason to expect Anonymous would carry out his instructions and do what he had suggested to the *Los Angeles Times*. So, Keys, ever eager to promote his own career interests as a digital journalist, pitched a scoop on Anonymous. On December 12, 2010, Keys emailed Brandon Mercer, "your ex-web producer infiltrated a group of hackers within the 'Anonymous' organization," and he predicted future operations against, among other entities, the *Los Angeles Times*. (GX 124.) He repeated this prediction in a conversation with that Mercer recorded at FBI direction. (GX 201.) But nothing happened. Perhaps growing frustrated, on December 14, 2010, Keys posted in an IRC channel used by Anonymous members, "Anyone interested in defacing FOX, LA Times?" (GX 610.)

One of the hackers finally did deface a *Los Angeles Times* story. The responsible editor at the Los Angeles Times regarded this as the most serious content-related security incident in his thirty-three years at the paper. (R.T. 297.) Keys finally got closer to getting what he had wanted out of his co-conspirators. The result at Tribune Company headquarters in Chicago was "panic," the personal involvement of the Chief Technology Officer, and a report to the Chief Executive Officer. (R.T. 506-507.) A large team of IT personnel spent that night locating loose super-user accounts and shutting down any other such back-door access points to Tribune Company's network. (R.T. 513-515.) Tribune Company's damage assessment had to be intensive because of the nature of the super-user credentials

that Keys had given Anonymous:

> It should be noted that there was trial testimony from Tribune Company employees responsible for running and/or repairing the Tribune's computer systems including Tom Comings, Tim Rodriguez, Jason Jedlinksi, Dylan Kuleza, and Armando Caro. These witnesses were assisted by multiple other Information Technology (IT) employees who worked on the response but did not testify. The witnesses discussed the difficulty of ensuring that all rogue accounts had been deleted, closing the "back doors" Keys had installed, and assessing whether the cyber attack had affected other parts of the Tribune's network including news archives, payment systems, and the systems that controlled the print editions of newspapers.

PSR ¶ 14. Keys denies and minimizes the evidence by denying creating "back doors" and characterizes his conduct as merely "an innocuous and short-lived edit to an *LA Times* story on tax cuts." (Def. Objs. at 8.) What was visible to the public is only a small part of the loss to Tribune Company. The guidelines and the CFAA itself anticipate this situation, and instruct that damage assessment and restoring the integrity of the system is "loss." U.S.S.G. § 2B1.1, application note 3(A)(v)(III); 18 U.S.C. § 1030(e)(11). Foreseeability is not even a factor for sentencing, but, of course, Keys as a former Tribune Company site administrator must have foreseen a vigorous response. Indeed, he warned Anonymous that Tribune Company deletes created super-user accounts. (GX 205-4.)

Apparently, Keys believed that the *Los Angeles Times* story defacement was not sufficient for his objective to "destroy" the newspaper or its parent company. On December 15, 2010, the next day, Keys tried to help sharpie get back in. Sharpie had a whole front page layout ready and had figured out how to "do a bunch of different layouts on different papers," and "have them all go live at the same time." (GX 506.) Keys's response was "hang on," and then an unhappy emoticon when he realized that his credentials had been deactivated. (*Id.*)

B. <u>The Investigation</u>

Matthew Keys was the initial suspect in this case and succeeded in deflecting suspicion away from himself. On December 12, 2010, two days before the *Los Angeles Times* defacement, the FBI requested that Brandon Mercer record his telephone conversation with Keys. (GX 201.) In June 2011, the FBI and the U.S. Attorney's Office had a discussion about whether Keys had wittingly or unwittingly assisted Anonymous in the *Los Angeles Times* hack. The agent wrote that Keys had seemed "genuinely baffled by allegations he perpetrated the intrusion" in this case, and "was otherwise candid

about his involvement with Anonymous." (6/6/2011 FBI Memorandum at MKP-0035802.) The FBI and the U.S. Attorney's Office agreed on three things that closed the Keys investigation: Keys was unwilling to provide information related to Anonymous hacking; Department of Justice regulations made it very difficult to get authorization to compel records from Keys; and without Keys, the proper venue for the case lay in Los Angeles. As a result, the case was transferred and its title was changed to delete Keys's name as a subject. (*Id.* at MKP-0035798, 35801.)

Six months later, on December 16, 2011, the Sacramento case agent reviewed chat logs seized in another one of the agent's investigations, which also involved Anonymous. (1/09/2012 FBI Memorandum at MKP-0035841.) The logs showed that Keys had had ample reason not to talk about Anonymous and the *Los Angeles Times* defacement. The reason was that Keys had instigated it. In the logs, members of Anonymous discussed among one another that Keys was AESCracked and had been the one who had given them the passwords for the *Los Angeles Times* and Fox 40. (*Id.* at MKP-0035841-43.) The agent then found AESCracked in the logs from the Ohio computer admitted at trial. (*Id.* at MKP-0035845.) This broke the case. Keys was again made the main subject and the case was returned to the Eastern District of California. (*Id.* at MKP-0035846.)

Keys was not targeted because he was a journalist. His employment and apparently sincere denials were together the reason Keys was at one point deleted as a subject.

C. The Motion to Suppress and the Trial

Matthew Keys was eventually indicted. Keys received all the process that he was due under the Constitution, the Federal Rules of Criminal Procedure, and the Rules of Evidence. He had excellent attorneys who brought credit to the legal profession through their hard work and agreement to accept this case *pro bono*. Keys litigated a motion to suppress the FBI's search and their two redundant recordings of the Mirandized confession.[1] Keys received discovery that included even the handwritten witness interview notes of the prosecutors. Finally, Keys, as was his right, received an eight-day trial before a jury of his peers, who were instructed not to convict unless they unanimously agreed that there was proof beyond a reasonable doubt. Keys confronted witnesses, put on what evidence he thought helped, and litigated various theories about the Computer Fraud and Abuse Act.

[1] Keys's motion relied, in part, on the FBI's decision to close the case against him in June 2011.

The jury evaluated eight days of trial evidence. There were logs from the CMS, files seized from Keys's own computer, logs from Overplay, logs from the chat room, the Cancer Man emails, a recording of Keys's conversation with Mercer, Keys's handwritten confession, and audio-recorded proof of Keys's oral statements to the FBI. (The complete transcript was filed by Keys at Dkt. 23-5.)

The evidence was overwhelming. The jury convicted Keys on all three counts.

D. Keys Lies and Promotes Cyncism about the Justice System

After the trial and without risking cross-examination under oath, Keys communicated extensively to the public in notable ways:

- He expressed contempt for the jury's verdict. On October 7, 2015, minutes after the verdict, he tweeted, "That was bullshit."
- He made false, self-serving statements about his conduct, his motives, and the investigation. He tried to cast himself as a reporter protecting sources and cast shame on the victim company for "being complicit" in what Keys cast as the justice system's outrage. On the day of the verdict, the *Los Angeles Times* reported:

> In an interview with The Times following his conviction, Keys used an expletive to describe the government's case against him and tweeted the same sentiment. He said prosecutors only went after him after he published information in 2011 that he gleaned from unnamed online sources, and refused to cooperate with federal investigators in a separate probe.
>
> . . .
>
> "It's wrong to call it a confession," he said. "Armed FBI agents who just pointed a gun at my face were telling me what to write."
>
> "They would love it if journalists who get background or go into dark places would play ball in criminal investigations," Keys said of prosecutors. "But we're under no obligation to do that. That's how we get out our stories – by protecting our sources."
>
> He drew similarities between the case against him and the government seizure of Associated Press phone records and the prosecution of a New York Times reporter for refusing to divulge a source, as examples. He had no part in the hacking of The Times site, in which the headline of an article was defaced, he said.
>
> . . .
>
> "Are you guys really that offended?" Keys asked a Times reporter.

"Shame on the Tribune Co. for being complicit in this." [2]

- On October 8, 2015, the following quote was observed in the *Sacramento News and Review* blog, "I did not commit the crime alleged," Keys wrote in an email. "I worked as a journalist observing a hacker group, and when I refused to comply with an FBI request to have my computer scanned for their investigation into Anonymous, I became a criminal suspect."
- On October 12, 2015, he tweeted, "There's no question I was targeted and falsely charged because of my work as a journalist."

III. ARGUMENT

A. The Offense was Serious Enough to Require a Substantial Prison Sentence.

Matthew Keys should be sentenced to reflect the seriousness of the crimes he committed. *See* U.S.C. § 3553(a)(2)(A). Keys used credentials and knowledge he obtained as a trusted network administrator to carry out, instigate, and guide attacks on journalists' ability to communicate with their viewers and readers. Keys created backdoor access points to the publishing system of a major American newspaper and then he persistently urged his co-conspirators to use the credentials to "target" and "destroy" that paper. To motivate his confederates, Keys told them about what the paper had published that they would not like. This was an online version of urging a mob to smash the presses for publishing an unpopular story. And Keys did it with an administrator's knowledge of the network and a journalist's understanding of what the profession is supposed to mean. To accomplish his angry, vengeful ends, Keys employed means that challenge core values of American democracy.

Brandon Mercer, former news director of Fox 40, was asked about his own personal interest in the outcome of this case and clearly stated:

> The reason . . . is because of the First Amendment. I feel if someone can hijack the means of publication, the means of communicating with the public, the means of doing our job as the press, if someone can hijack that and do what they will with it, the First Amendment is in jeopardy and the freedom of the press is in jeopardy, and that cannot be done with impunity.

[2] http://www.latimes.com/local/lanow/la-me-ln-matthew-keys-convicted-hacking-la-times-20151007-story.html. The article was updated to include the undersigned prosecutor's post-verdict statements made in direct response to Defendant's lies.

(R.T. at 206.) The pecuniary harm in this case is accurately calculated in the PSR. But it is only part of the story. Keys's attack on Tribune Company's network caused pecuniary harm, albeit not as much as Keys had hoped. But more important was something not reflected in the guidelines. This was not just an attack on an online merchant for profit. It was an attack on a newspaper for what it printed.

B. Keys's Personal Character Does not Favor a Lenient Sentence.

In a way, one can at least *understand* Keys's desire to harm Tribune Company. Plenty of people have workplace incidents that lead them to hate their employer. But it is much harder to understand how indifferent Keys was toward the collateral damage he caused in the homes of total strangers. Keys knew that a lot of Fox 40 Rewards participants had uploaded their credit card information to the channel, and he intentionally wrote messages to frighten them about misuse of that information. (GX 107.) It worked. Viewers called the station worried about the security of their bank accounts and credit cards. (R.T. 197-198.)

"Worried" would be an understatement for the emotions of at least one Fox 40 viewer. The Court will recall that Mercer told "Cancer Man" that Mercer had just talked down a tearful elderly woman who had been having a "panic attack" over the emails while her husband was in kidney failure. The Court ordered this and Keys's reaction redacted before it went to the jury. The Rule 403 exclusion meant that the Court thought the unredacted email would have created a substantial risk that the jury might read it and return a verdict based on something other than the elements of the offense. The Government respects the Court's ruling. The way Keys reacted shows he is a different and worse kind of person. Keys ridiculed the station for "reporting to the old folks home" and casually passed judgment on the poor woman for having her priorities "in the wrong place there." (GX 1001.) Keys's haughty, cold reaction to that woman's suffering was the other reason that Mercer said he came to take a personal interest in the outcome of this case. (R.T. at 189-190.) The Court should sentence to reflect the characteristics of the Defendant. *See* 18 U.S.C. § 3553(a)(1). Keys's characteristics include narcissism and an arrogant indifference to the suffering of innocent and vulnerable people.

C. Keys's Public Statements to Undermine Confidence in the Jury's Verdict Favor a Stronger Sentence to Promote Respect for Law.

Keys's sentence must also be sufficient to promote respect for law. *See* 18 U.S.C.

§ 3553(a)(2)(A). It is exceptionally rare to see a defendant engage in an after-verdict press campaign to undermine public confidence in the jury's verdict. It is a direct attack on the work of the jury and the validity of the verdicts. It undermines respect for law at a time when the public seems more willing to credit strongly worded criticism of traditional institutions. But there was a trial and there was evidence. The Court should send a strong message regarding what happened in this trial and what the Court thinks of Keys's statements. In this context, there is no substitute for the Court's pronouncement of a strong sentence and clear reasons. The criminal jury trial, like the free press, is one of the most important institutions of our democratic system. After the verdict, Keys showed himself perfectly willing to undermine yet another institution of democracy because he does not want people to think that he did what the evidence overwhelmingly proved he did.

D. Network Administrator Misconduct Must be Answered with a Deterrent Sentence.

A network administrator's attack on a network requires an adequately deterrent sentence. *See* 18 U.S.C. § 3553(a)(2)(B). This kind of insider misconduct is a serious threat to computer security. All over the economy, network administrators are trusted to safeguard sensitive information and maintain essential systems. Some of them probably hate their bosses and the CFAA functions in part to deter insiders from damaging systems. Matthew Keys knew all about the insider threat. His "Going Rogue" email helps demonstrate how deterrent interests weigh strongly against a sentence too far off the guidelines range:

> There is a new urgency to addressing information security inside corporations and a reminder of its limits when confronted with a determined insider.
>
> At risk are companies' secrets – e-mails, documents, databases, and internal websites that are thought to be locked to the outside world. Companies create records of every decision they make.
>
> Although it is easy, technologically, to limit who in a company sees specific types of information, many companies leave access too open. Despite the best of intentions, mistakes happen and settings can become inadvertently broad, especially as networks grow more complex with reorganizations and acquisitions.
>
> Even when security technology is doing its job, it is a poor match if someone with legitimate access decides to go rogue.

(GX109.)

E. Sentencing Uniformity Favors a Sentence at or Close to the Guidelines Range.

Keys has already complained that the PSR recommends a sentence longer than that received by another hacking defendant who pleaded guilty in another district. The Ninth Circuit has an answer for this kind of argument:

> The mere fact that [Keys] can point to a defendant convicted at a different time of a different [computer crime] and sentenced to a term of imprisonment shorter than [Keys's] does not create an 'unwarranted' sentencing disparity. For one thing, we aren't presented with the records in the cases on which [Keys] relies when he argues that other [computer crime] defendants got off better than him. Moreover, sentencing disparity is only one factor a court considers in crafting an individualized sentence under § 3553(a).

United States v. Treadwell, 593 F.3d 990, 1012 (9th Cir. 2010). A broader survey of computer crime cases is of no more value. "A district court need not, and, as a practical matter, cannot compare a proposed sentence to the sentence of every criminal defendant who has ever been sentenced before. Too many factors dictate the exercise of sound sentencing discretion in a particular case to make the inquiry Treadwell urges helpful or even feasible." *Id.* The way to promote uniformity is to correctly calculate and give due weight to the guidelines. That is their purpose. *Id.*

Keys may be able to point to computer crime cases where defendants pleaded guilty and received sentences lower than the one recommended in this case. These cases are extremely expensive and time-consuming to prosecute, and it would not be surprising if a raft of computer crime defendants have received lenient sentencing recommendations in return for saving the Government's resources for use in other cases. Those defendants are not similarly situated and that is not an *unwarranted* disparity. *See United States v. Carter*, 560 F.3d 1107, 1121 (9th Cir. 2009) (defendants who cooperate are not similarly situated), and *United States v. Monroe*, 943 F.2d 1007, 1017 (9th Cir. 1991) (defendant who went to trial was not similarly situated with defendant who had participated in same conduct but had a plea agreement to lesser charges). The Supreme Court recognizes that plea agreements necessarily flow from "the mutuality of advantage" between prosecutors and defendants. *See United States v. Goodwin*, 457 U.S. 368, 379 (1982). The Ninth Circuit knows how important that system is and teaches,

> When a defendant voluntarily chooses to reject or withdraw from a plea bargain, he retains no right to the rejected sentence. Having rejected the offer of a lesser sentence, he assumes the risk of receiving a harsher

> sentence. If defendants could demand the same sentence after standing trial that was offered in exchange for a guilty plea, all incentives to plead guilty would disappear. Defendants would lose nothing by going to trial. The reality of plea bargaining is that once the defendant elects to go to trial, all bets are off.

United States v. Carter, 804 F.2d 508, 513-514 (9th Cir. 1986) (internal citations and quotations omitted), *see also United States v. Vasquez-Landaver*, 527 F.3d 798, 805 (9th Cir. 2008).

If the Court is to compare this case to others, it should consider network crimes in the broadest sense. This kind of crime exploits any kind of vulnerability in a network that people rely on to convey information and assets among one another. Network criminals harm individuals without facing them and harm the economy generally by threatening the linking infrastructure upon which modern activity relies. Postal theft has been a network crime for a very long time. There is a whole chapter of Title 18 dedicated to protecting the postal system. Each theft of mail matter is is a five-year felony. *See* 18 U.S.C. § 1708. The purpose of these theft statutes is to protect "the mails" by extending federal protection to the matter deposited in the system. *Thompson v. United States*, 202 F. 401, 405 (9th Cir. 1913); *McCowan v. United States*, 376 F.2d 122, 124 (9th Cir. 1967).

Today's defendants convicted of yesterday's network crime generally commit the offense out of drug-addicted desperation. They find vulnerable mail boxes, harm customers, and impose costs on the network. But few mail thieves manage to affect as many people for as much pecuniary harm as did Matthew Keys. Such defendants are routinely sentenced to imprisonment and it is completely unremarkable.

What is remarkable is Keys's insistence that his crime does not merit a years-denominated prison sentence. Keys's network crime caused far more damage than even a very large-scale postal theft. The fact that Keys carried this out as a formerly trusted insider, digitally, while covering his tracks through a foreign proxy server, makes him more culpable, not less. The Defendant's articulateness and his out-sized, narcissistic sense of specialness should not sway the Court into treating him more favorably.

IV. CONCLUSION

Matthew Keys committed a serious crime that requires strong deterrence. In his crime, he targeted an institution that our Democracy has a special interest in protecting. In his post-verdict defiance, he targeted the justice system itself. All of this conduct merits strict punishment and indicates

a character that warrants the same. The United States requests a sentence of five years imprisonment.

Respectfully submitted,

Dated: March 9, 2016

BENJAMIN B. WAGNER
United States Attorney

By: /s/ MATTHEW D. SEGAL
MATTHEW D. SEGAL
Assistant United States Attorney