JASON S. LEIDERMAN, SBN 203336
LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280
jay@criminal-lawyer.me

TOR EKELAND, PRO HAC VICE
MARK JAFFE, PRO HAC VICE
tor@torekeland.com
mark@torekeland.com
TOR EKELAND, P.C.
195 Plymouth Street
Brooklyn, NY 11201
Tel: 718-737-7264
Fax: 718-504-5417

Pro Bono Attorneys for Defendant
MATTHEW KEYS

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

THE UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW KEYS Defendant.	Case No.: 2:13-CR-00082 (KJM) **SENTENCING MEMORANDUM** Date: MARCH 23, 2016 Time: 9:00 am Place: Courtroom 3

Defendant MATTHEW KEYS ("Defendant" or "Keys" or "Matthew") states the following for the Court's consideration in determining his sentence:

INTRODUCTION

In late 2010 the loosely knit hacking collective Anonymous was in the news. Anonymous launched cyber-attacks against Visa, MasterCard, PayPal and Amazon.com. These attacks were political protests supporting Julian Assange and WikiLeaks. WikiLeaks had published State Department cables on its site and because of this, the companies refused to process donations for WikiLeaks.

Because of this, numerous reporters sought access to Anonymous. Matthew Keys was one of them. Matthew gained access to a top level Anonymous Internet chat room, then known as Internet Feds. In the room were hackers that would become famous, infamous, celebrated, prosecuted and ultimately sentenced by either the US, English or Irish courts. The period of 2010 through early 2012 was one of recklessness and whim on the Internet – the Internet had arrived in a new way in popular culture. Articles about the people Matthew Keys met in Internet Feds now number over 9,000. Recently a play at the Royal Court Theater in London, "Teh Internet is Serious Business (sic)" depicted the exploits of the denizens of Internet Feds – Kayla, T-Flow (known as Chronom in Internet Feds), Sabu (cast as the villain), PwnSauce and other Internet Feds participants. Internet Feds turned into its more famous successor-LulzSec. Matthew Keys had access to Internet Feds only for a short while, before the transformation into Lulzsec. His conviction rests upon this time in Internet Feds, essentially for the passing of a username and password to the content management system for the Los Angeles Times resulting in minor changes to a minor website story on tax cuts that were easily restored in roughly 40 minutes. For this he faces a statutory maximum of 25 years in jail and $750,000.00 in fines. He has been on supervised release for this entire case without any violations, has appeared every time he was required, and has respected every order of this Court. Therefore, for the reasons stated below, he asks the Court to impose a non-custodial sentence.

STATEMENT OF THE CASE

This case stems from minor edits to the headline of a trivial story on the Los Angele Times website on December 14, 2010. That day, using the Los Angeles Times/Tribune Company's content management system ("CMS"), the user "ngarcia" altered a few words in a latimes.com story on tax cuts.

Because of this, Matthew was convicted of one count of conspiracy to violate the Computer Fraud and Abuse Act ("CFAA"), in violation of 18 U.S.C. §§ 371 and 1030(a)(5)(A); one count of

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

knowingly transmitting a code with the intent to cause damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A); and one count of attempt to transmit a code with the intent to cause damage to a protected computer in violation of 18 U.S.C. § 2 and 1030(a)(5)(A).

For this he faces a maximum sentence of 25 years in jail, $750,000 in fines, 9 years of supervised release, and criminal forfeiture. *U.S. v. Keys*, Superseding Indictment, 2:13-CR-00082 (Dec. 4, 22 2014) (ECF # 44). (*See generally,* Pre-Sentence Report, ECF No. 127 (PSR).)

The PSR recommends an unconscionable sentence of 87 months and a 2-year term of supervised release. Even the government believes this is too much:

> The statutory maximum for Keys's crimes is 25 years, but in a statement given after the trial, a spokesperson for the US Attorneys Office said Keys would likely face less than five years.
>
> "While it has not been determined what the government will be asking the court for, it will likely be less than 5 years," the spokesperson said.
>
> "This is not the crime of the century," [United States Attorney and the Prosecutor in this case Matthew] Segal said, adding that nonetheless Keys should not get away with his acts. At minimum, he may receive probation.[1]

MATTHEW KEYS' BIOGRAPHY

Matthew Keys has pursued journalism most of his life. A cursory glance at his record shows an intense dedication to bringing stories of importance to light — sacrificing his time and resources, and in some cases, his money and health.

In recent years, Matthew's sacrifices have paid off in the form of impactful journalism that has received national attention. His stories have encouraged discourse, influenced policy and won the attention and accolades from his peers in the industry, public interest groups and even law enforcement officials.

His desire to pursue stories began in elementary and middle school where he both created and served as editors to two school news bulletins. In high school, he was one of eight contributors toward

[1] Sarah Jeong, "Former Reuters Journalist Matthew Keys Found Guilty of Three Counts of Hacking," available at http://motherboard.vice.com/read/former-reuters-journalist-matthew-keys-found-guilty-of-hacking-faces-25-years

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

his school's first long-form newspaper and later served as a news editor for it. At the age of 16, he was the youngest journalist to serve as a correspondent to the homecoming of former prisoners of war from the 507th Maintenance Company at Fort Bliss, Texas during Operation Iraqi Freedom. During the homecoming, he was interviewed by reporters and photographers from other news organizations, including Amber Rupinta of WCAU-TV (now at WTVD) and freelance journalists working for Harpo Studios, the television production company run by Oprah Winfrey. He was also one of two students to work on the television broadcast team, and as a senior was drafted to help instruct a handful of journalism classes at his school.

In college, he started a blog, RadioMatthew.com, which initially began as a space to write on personal topics but later grew to become an influential digital publication covering media and local news in the Sacramento area. His readers included newspaper reporters, television anchors and broadcast producers throughout the area. His writings led Brandon Mercer, the former news director at KTXL FOX40, to hire him as the station's first web producer. Mr. Keys left college in 2008 to focus on his job at FOX40 full time. He subsequently closed his blog, which prompted a newspaper article in the widely-read Sacramento Bee.[2]

A. <u>At FOX40 News</u>

Matthew's first job was to transform FOX40's website — which until that point had been used as a promotional platform for the station — into a local news publication. He was instructed to build a website that incorporated both written stories and videos from various sources, including the station's own news broadcasts, the Associated Press, Reuters News, CNN, the FOX News Channel and other Tribune media properties. He was asked to find new and compelling ways to promote the station's news content so that it would reach as many local viewers as possible and compete against three other broadcast news properties in the Sacramento television market. He was asked to grow the FOX40 website to one million page views[3] within a one-year period.

---

[2] Rachel Leibrock. "RadioMatthew Calls It a Day." *The Sacramento Bee* (Oct. 14, 2013), available at http://blogs.sacbee.com/ticket/archives/2008/05/radiomatthew-ca.html.

[3] A "page view" is a metric used to measure the amount of traffic, or viewership, a website receives. One page view is the equivalent of a person viewing a page on a website once. Page views are sometimes colloquially referred to in the online industry as "clicks."

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Matthew was hired by FOX40 in June 2008. The station used Adobe software called Omniture to measure the amount of traffic their website received, with measurements available in hourly, daily, weekly, monthly and yearly increments. When Matthew started, FOX40's website received just under 300,000 monthly page views. By November 2008, this figure grew to over 400,000 page views; in April 2009, FOX40's website received more than one million page views, and registered another six million the following month. The goal that Matthew was tasked to achieve — one million monthly page views within one year — was completed in ten months, and was sustained throughout the remainder of his career with the station.[4]

Mr. Keys achieved the goals set by his employer by experimenting with new forms of storytelling, emerging technologies and by adopting an aggressive, play-to-win attitude. Two months into his employment, he registered Twitter and Facebook accounts for FOX40 using his personal e-mail accounts as an experiment in reaching new audiences through the Internet. Despite initial concerns by his direct supervisor over the approach, Mr. Keys built a healthy following on both social media platforms — because of his efforts, FOX40 was the first station in Northern California to have a presence on Twitter, and his work on Facebook was emulated by the station's competitors in the following months.

He also regularly trained other employees — including reporters and photographers — on the best social media practices to maximize exposure and attract new followers and viewers. Today, many of the reporters he trained have healthy followings on their personal and professional social media accounts.

While at FOX40 News, Matthew covered some of the most-memorable stories of his career. In March 2009, he led a station-wide initiative to create a news website separate from FOX40.com that published stories and information on a missing 8-year-old girl named Sandra Cantu. Matthew successfully lobbied the station to run the website as an advertisement-free public service while at the same time committing both human and financial capital to the effort. Members of the community used the website to learn about the latest developments, get information on contacting law enforcement and

[4] *See* Page Views Report 2008, available at https://www.dropbox.com/s/xujyvdpe0p1b7kz/FOX40-Metrics-2.pdf?dl=0.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

organize search rallies. A company called ButtonWorks created shirt buttons featuring the address of the website, and Home Depot donated thousands of fluorescent-colored missing posters again emblazoned with the address of the website. The website was turned into a digital memorial when it was tragically discovered that Cantu had been murdered by her former Sunday school teacher. At the suspect's murder trial, Cantu's family testified that they learned about developments in the search and subsequent arrest by watching FOX40.

In September 2009, a wildfire broke out near Auburn, California. The so-called "49 Fire"[5] erupted on a Saturday when Matthew and other newsroom employees were typically not at the station. After learning about evacuations in the community, he not only went to the station on his day off, but provided up-to-the-minute coverage of the fire well into the next morning. He remained at the station until the following afternoon, providing more than 18 hours of coverage. He and others at the station received e-mails from evacuees and concerned loved ones throughout the country praising FOX40's continuous updates on-air, online and on social media.

As part of his job duties, Matthew regularly communicated with law enforcement officials in order to provide accurate and timely information to FOX40's news audience. He also provided law enforcement information that led to criminal arrests. In December 2009, while researching exercise equipment on Craigslist, he came across a listing where someone was trying to illegally sell prescription pain medication. Matthew contacted the seller and was able to get an e-mail address and a phone number. He researched the phone number and came across a social media profile where the seller claimed to have ties with the Norteno[6] gang. He collected his research and contacted general assignment reporter Rowena Shaddox, enlisting her help to contact local law enforcement.

Shaddox and Matthew contacted Norm Leong, then a sergeant and police spokesperson with the Sacramento Police Department. With FOX40 present, Sacramento police organized a sting to apprehend the individual responsible for the attempted illegal transaction. Police also learned that the

[5] According to statistics released by Cal Fire, the 49 Fire burned over 340 acres, destroyed 63 homes, and significantly damaged six businesses. Hundreds of people were evacuated from affected communities. The cause of the fire remains unknown. *See* Incident Information, Forty Nine (49) Fire, Cal Fire Website, available at http://cdfdata.fire.ca.gov/incidents/incidents_details_info?incident_id=380.

[6] THE omnibus Northern California prison gang; Nortenos control all street gang activity in Northern California.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

suspect, who was a juvenile, was wanted for a string of local burglaries and was also attempting to sell stolen merchandise. The police department credited the arrest to the initial research performed by Matthew, Shaddox and FOX40.

Matthew's work diligently at FOX40. As the station's sole employee for online and digital initiatives, he often worked at night and on weekends from his home. The station encouraged this work by providing him with a mobile Internet card, and he was expected to check his e-mail and answer the phones when he was off-the-clock.

As a consequence of his long hours and the accompanied stress, he suffered from severe, cystic acne and was prescribed the potent drug Accutane on two occasions. He was also diagnosed in August 2010 with mild insomnia and prescribed the sedative Trazodone.

That same month, he was told during a meeting with his supervisor that the station did not feel he was ready to take on managerial role, and that they would be looking to hire someone to oversee the station's website and other digital initiatives. Discouraged by the lack of opportunity at the station in spite of his achievements, he left the station following a newsroom dispute in October 2010.

After FOX40

From late October 2010 to April 2011, Matthew worked as a self-published freelance journalist, covering stories he felt would be both interesting, important and impactful. He used his knowledge and experimentation with emerging social medium platforms to showcase his newsgathering and storytelling abilities.

In December 2010, in pursuit of a story on Anonymous, he was invited into the Internet chat room Internet Feds. His reporting helped the public better learn and understand who Anonymous was and what their intentions were at the time. Information he learned from his observation of the group was used by reporters for the PBS NewsHour, Gawker, and for a book on Anonymous authored by Forbes reporter Parmy Olson. His research would also be the focal point of a story published by Reuters in March 2012.

In January 2011, he covered the shooting of former U.S. Representative Gabrielle Giffords. He utilized the social platforms Twitter and Tumblr to deliver short updates on the shooting and subsequent investigation in real-time for more than three weeks. He used the same technique to cover social unrests

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

in the Middle East and a powerful earthquake and subsequent tsunami in Japan. He was profiled by the website AdWeek[7] for his work on those stories, and was nominated for an Online News Association award for his storytelling on the Japan earthquake.

His use of social media to cover stories impressed colleagues across the country, and it led to two additional job opportunities: In May 2011, he was hired as a weekend news producer for KGO-TV in San Francisco, and seven months later he accepted a different job working as a journalist for the Reuters News Service in New York City. While at Reuters, he covered a number of significant stories of national and international interest, including the 2012 London Olympics, the Colorado movie theater shooting, the presidential election, the Sandy Hook massacre and the appointment of Pope Benedict XVI. And despite living within the impact zone, he provided rolling coverage of Hurricane Sandy in November 2012 from his home until his electricity went out.

During his time at Reuters he was asked to provide commentary and insight on a number of emerging digital media trends and technologies. The Huffington Post declared him a must-follow journalist for news on Facebook,[8] Time Magazine named him one of the 140 best Twitter feeds to follow in 2012,[9] and the website Journalism.co.uk declared him one of the 100 people every journalism student should follow.[10]

Reuters terminated Matthew as an employee in early 2013 after his indictment. Despite significant resource and financial hardships since then, he remained committed to journalism and continued covering important news stories. And, even while under indictment, some of his stories had a significant impact on public discourse and policy.

In June 2013, the Guardian and Washington Post newspapers broke numerous stories disclosing clandestine — and in some cases, illegal — wiretapping and surveillance operations by the National

---

[7] , Ethan Klapper "Meet Producer Matthew, Aggregation Journalist." *AdWeek* (Mar. 21, 2011), available at http://www.adweek.com/fishbowlny/meet-producer-matthew-keys-aggregation-journalist/243891.

[8] "50 People in Media You Should Subscribe to on Facebook" The Huffington Post (Apr. 30, 2012), available at http://www.huffingtonpost.com/2012/04/30/facebook-subscribe-suggestions-50-in-media_n_1464571.html#gallery/223172/29.

[9] Amy Lombard "The 140 Best Twitter Feeds of 2012" Time (Mar. 15, 2012), available at http://techland.time.com/2012/03/21/the-140-best-twitter-feeds-of-2012/slide/matthew-keys/.

[10] Sarah Marshall "100 Twitter Accounts Every Journalism Student Should Follow" journalism.co.uk (Sept. 24, 2012), available at https://www.journalism.co.uk/news/100-twitter-accounts-every-journalism-student-should-follow/s2/a550471/.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Security Agency (NSA). In November 2013, under a presidential order, the Foreign Intelligence Surveillance Court released a trove of documents related to their approval of some NSA operations. Matthew reviewed those documents and determined that between the years 2005 and 2011, every request by the NSA to conduct surveillance had been approved by the court[11]. This research was later used for journalist Glenn Greenwald's book *No Place to Hide*. Greenwald credited Keys for his research.[12]

In mid-2013, a hacker group known as the Syrian Electronic Army made international headlines after compromising numerous social media accounts used by news websites. While news publications widely reported what the Syrian Electronic Army had done, few looked deeper into who the group was or what their intentions were. In May 2013, Matthew became the first journalist to conduct an interview with a representative of the Syrian Electronic Army.[13] In December 2013, he produced the first live conversation[14] with the same representative. His research helped de-bunk widely-reported assertions that the hacker group was tied to the Syrian government and gave the public greater insight into the collective and their ambitions.

In November 2013, Matthew obtained radio dispatches related to a fatal incident involving a BART commuter train and two maintenance employees weeks earlier. His story revealed that there were numerous problems involving both the train "lookout" method and the radio equipment used by the workers that day. The audio tapes Matthew obtained were widely cited by local media, including the San Francisco Chronicle[15]. They were also solicited from him for a pending lawsuit filed by one of the family members of a BART employee killed that day. Matthew provided the tapes to the family upon their request, and absorbed the expenses in doing so.

---

[11] Matthew Keys, Twitter Feed (7:23am Nov. 19, 2013), available at https://twitter.com/MatthewKeysLive/status/402774028898672640.
[12] Glenn Greenwald "No Place to Hide: Booknotes", available at http://glenngreenwald.net/#BookNotes.
[13] Matthew Keys "A Conversation with the Syrian Electronic Army" The Desk (May 14, 2013), available at http://thedesk.matthewkeys.net/2013/05/a-conversation-with-the-syrian-electronic-army/.
[14] *Id* at http://thedesk.matthewkeys.net/2013/12/a-live-conversation-with-the-syrian-electronic-army/.
[15] Demian Bulwa "BART Workers on Tracks Don't Get Train Warnings" SFGATE (Oct. 21, 2013), available at http://www.sfgate.com/bayarea/article/BART-workers-on-tracks-don-t-get-train-warnings-4914319.php.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

In March 2014, he began a 14-month investigation into clandestine cellphone surveillance devices used by law enforcement known as a "StingRay." During his investigation, he successfully landed an on-the-record interview with a police spokesperson in which the officer admitted the devices were used in numerous criminal investigations. The admission countered assertions at the time by federal agents that Stingrays were limited in use to homeland security investigations. His report on the acknowledgement was used in a letter filed by the American Civil Liberties Union[16] on the topic several months later.

Matthew's investigation concluded when the Federal Communications Commission released a heavily-redacted manual related to the StingRay device.[17] Although the manual contained little additional insight into how law enforcement obtained or used them, it was the first public acknowledgement by the FCC of the device's existence. Matthew filed more than two dozen stories on the topic during his investigation, and his research and reporting was cited by Vice News[18], Slate[19], the International Business-Times[20] and others.

In August 2014, Matthew investigated comments made by then-Ferguson Police Chief Thomas Jackson as to why he released a surveillance tape depicting slain 18-year-old Michael Brown, Jr. minutes before he was shot by a Ferguson police officer. Jackson told reporters at a press briefing that the tape was released pursuant to numerous open records requests filed by members of the media. After researching, Matthew discovered that the Ferguson police had received no specific requests for the tape from any reporter. In September, Matthew broke the story that Jackson had lied about receiving

---

[16] Letter form Laura W. Murphy, Director, ACLU Washington Legislative Office, to The Honorable Tom Wheeler, Chairman, FCC (Sept. 17, 2014), available at https://www.scribd.com/doc/240893938/ACLU-calls-on-FCC-to-investigate-Stingray-manufacturer-Harris.

[17] "Exclusive: Stingray Maker Asked FCC to Block Release of Spy Gear Manual" the blot magazine (Mar. 26, 2015), available at http://www.theblot.com/exclusive-stingray-maker-asked-fcc-to-block-release-of-spy-gear-manual-7739514.

[18] Lucy Steigerwald "Everything We Know About the Singray, the Cops' Favorite Cell Phone Tracking Tool" Vice (Apr. 13, 2015), available at http://www.vice.com/read/everything-we-know-about-the-stingray-cops-favorite-cell-phone-tracking-tool-413.

[19] Lily Hay Newman "FCC Finally Releases (Heavily Redacted) Manual for Controversial Surveillance Device" Slate (Mar. 27, 2015), available at http://www.slate.com/blogs/future_tense/2015/03/27/fcc_releases_heavily_redacted_stingray_manual_to_the_blot.html.

[20] Jeff Stone "Sweeping 'Stingray' Surveillance Technology Has No Restrictions, Despite Serious Privacy Concerns: Police" International Business Times (Jul. 7, 2014), available at http://www.ibtimes.com/sweeping-stingray-surveillance-technology-has-no-restrictions-despite-serious-privacy-1631448.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

requests for the tape, calling into question the Ferguson Police Department's motive for releasing it. His report received national attention as was covered by the Huffington Post[21], MSNBC[22] and others. Matthew was commended by Brown's family attorney Benjamin Crump for his investigation, and his story was used as the foundation of a letter urging Jackson to resign.[23]

Finally, in June 2015, a startup news organization called Grasswire hired Matthew to be a managing editor. In November 2015, he began an investigation into a surveillance tape that depicted the beating of a suspect by Alameda County, California sheriff's deputies at the end of a pursuit. The police severely beat that suspect, later identified as Stanislav Petrov.

While working on the investigation, Grasswire ran into financial difficulties. Two days before Christmas, the website's editor-in-chief announced that all paid staffers were to be laid off effective immediately. Despite losing his job, and at considerable financial expense, Matthew published the findings of his two-month investigation into the Petrov beating.[24] His story contained numerous previously-undisclosed facts, including the identities of the two deputies who appeared on the surveillance tape. His story was cited by the San Francisco Chronicle[25] and other newspapers[26], and his investigation was praised by Alameda County Public Defender Brendon Woods.[27]

Despite his indictment, Matthew continued to report on matters of crucial public interest, bringing to light important facts on critical matters that, without his reporting, may never have seen the light of day. Taken as a whole, his commitment to journalism also demonstrates a commitment to public service. At a time when other journalists concern themselves with which burrito restaurant a

---

[21] Simon McCormack "Ferguson Police Chief Lied About Why He Released Alleged Michael Brown Robbery Tap: Report" The Huffington Post (Sept. 6, 2014),available at http://www.huffingtonpost.com/2014/09/05/ferguson-chief-lied-about-michael-brown-tape_n_5773420.html.

[22] All In With Chris Hayes, NBC New Show, Transcript (Sept. 5, 2014), available at http://www.nbcnews.com/id/56008773/ns/msnbc-all_in_with_chris_hayes/.

[23] Jackson resigned as Ferguson's police chief eight months later.

[24] Matthew Keys, "Grasswire Investigates: Alameda County Deputies Involved in November Beating Named" Grasswire (Dec. 24, 2015), available at https://medium.com/grasswire-blog/grasswire-investigates-alameda-county-deputies-involved-in-november-beating-named-d0ca44d399e2#.luij65y4a.

[25] Vivian Ho, Twitter Feed (6:59pm Dec. 24, 2015), available at https://twitter.com/vivianho/status/680176029093072898.

[26] Katrina Cameron, "Alameda County Deputies Involved in San Francisco Beating Identified" Times#Standard News (Dec. 24, 2015), available at http://www.times-standard.com/general-news/20151224/alameda-county-deputies-involved-in-san-francisco-beating-identified/1.

[27] Brendan Woods, Twitter Feed (3:20am Dec. 25, 2015) available at https://twitter.com/BrendonWoodsPD/status/680302139114041344.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

presidential candidate patrons[28] or the numerous antics of a real estate mogul-turned-politician,[29] it someone who has dedicated serious personal and professional effort, sometimes at his own considerable expense, to research and publish impactful stories on topics that matter to the public, should not be incarcerated. If he were to be sentenced to any prison term, people in positions of authority who will go unchecked and stories of public importance that will go untold.

BACKGROUND[30]

In the latter part of 2010, Matthew Keys entered an Internet chat room populated by high-level and highly skilled hackers belonging to the loosely knit hacking collective "Anonymous." He was invited in as a journalist. He had been in another, larger chat room where people were discussing large scale attacks on Visa, Master Card, Amazon and PayPal as revenge for a banking blockade on the whistleblowing site WikiLeaks. There was no bigger Internet news in early December 2010 and as a journalist, Matthew wanted in on the ground floor of the story.

Though the hacking world, the language and the activities of Internet chat rooms were all foreign to Matthew, reporting was not. In 2004, at the age of 17,[31] Mr. Keys started his own news network. At present, he has his own news network with numerous subscribers and followers. He has spent night and day since he was 17 dedicating himself to the pursuit of delivering the news to the public. Now, he faces an end to any reporting for potentially greater than 7 years, as recommended by the PSR.

The charges in this case stem from minor edits to the headline of a story on the Los Angeles Times website on December 14, 2010. That day, using the Los Angeles Times/Tribune Company's

---

[28] Maggie Haberman, "Hillary Clinton, Just an Unrecognized Burrito Bowl Fan at Chipolte" New York Times (Apr. 13, 2015), available at http://www.nytimes.com/2015/04/14/us/politics/on-the-road-hillary-clinton-stops-for-lunch-at-chipotle-and-goes-unrecognized.html?_r=0.

[29] Maggie Haberman "Donald Trump did Stay at a Holiday Inn Express on Friday Night" New York Times (Jan. 24, 2016), available at(http://www.nytimes.com/politics/first-draft/2016/01/24/donald-trump-did-stay-at-a-holiday-inn-express-on-friday-night/.

[30] All facts relating to the hackers discussed throughout this brief have been checked the person at issue except for: Hector Monsegur (A journalist familiar with Monsegur verified Monsegur's present employment), Ryan Ackroyd, Ryan Cleary (though their co-defendants verified the facts related to both the case and to them personally), some of the PayPal 14, all but one of the Payback 13, Christopher Weatherhead's co-defendants in the English PayPal case, John Borell, Jon Cowden (facts verified by his girlfriend as correct), Jeremy Hammond (though Attorney Leiderman consulted on the case and knows the facts to be true), and Cody Kretsinger (due to Leiderman's representation of Royal Rivera, Kretsinger's co-defendant, Leiderman knows the facts to be accurate).

[31] The Skylark Network. *See* http://skylark1348.tripod.com/id12.html

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

content management system ("CMS"), the user "ngarcia" altered a paragraph of an latimes.com story. The article's headline, deck and byline originally appeared as follows:

> Pressure builds in House to pass tax-cut package
>
> House Democratic leader Steny Hoyer sees 'very good things' in the tax-cut deal, which many representatives oppose. But with the bill set to clear the Senate, reluctant House Democrats are feeling the heat to pass it.
>
> By Lisa Mascaro, Tribune Washington Bureau[32]

After the minor edits by ngarcia, the article's title and byline allegedly read:

> Pressure builds in House to elect CHIPPY 1337
>
> House Democratic leader Steny Hoyer sees 'very good things' in the deal cut which will see uber skid Chippy 1337 take his rightful place, as head of the Senate, reluctant House Democrats told to SUCK IT UP.
>
> By CHIPPYS NO 1 FAN, Tribune Washington Bureau

No alterations were made to the text of the actual article, meaning that one who proceeded past the joke headline received the proper information about Steny Hoyer and the Democrats' tax-cut deal. Website administrators restored the original in less than 40 minutes. For this, Matthew was convicted of three felony counts of violating the Computer Fraud and Abuse Act (CFAA).

Count one, the conspiracy under 18 USC § 371 in this case was largely due to logs showing that AESCracked passed credentials to an Anonymous member named "Sharpie" and while saying "go fuck some shit up."

Count two, transmission of a code with the intent to cause unauthorized damage to a computer in violation of 18 U.S.C. 1030(a)(5)(A) also rests upon the evidence at trial that Matthew passed login credentials to the Tribune Co. content management system and the statement: "go fuck some shit up."

Count three, attempt to cause damage to a computer, rested again on the same basic set of facts.

Sprinkled in for prejudicial flavor at trial were emails from email addresses based on "X-Files" characters to Matthews' former employer, FOX40 in Sacramento. They made vague threats about

[32] The original article is still available on the Los Angeles Times website, *See* Lisa Mascaro, "Pressure builds in House to pass tax-cut package." Los Angles Times (December 14, 2010), available at http://articles.latimes.com/2010/dec/14/news/la-pn-hoyer-tax-vote-20101215

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

exposing that FOX40's give-away contests were fixed and that the computer security of the station was suspect.

Internet Feds and LulzSec, 2010-1011: Popular Culture and the Hacktivist as Celebrity

The CFAA violations and U.K.'s Computer Misuse Act (the U.K. analogue of the CFAA) violations committed by the members of "Internet Feds," later to be named "LulzSec," shed light on the instant crime as well as the times that this crime occurred. September 2010-March 2012 was marked by an explosion of aberrant computer hacking behavior, the likes of which the world had never seen; a behavior that became infectious, a matter of media curiosity, and behavior that was roundly cheered by the online community. It is important to see the zeitgeist of this period for what it is – the world being swept up in a world marked by a groupthink of hacking madness. The acts of this period had a social and political significance. They also spoke to a herd mentality – those that got swept up in the September 2010 to March 2012 era played to a popular and new ethos. The Internet was awash in hacker news. There was tremendous competition for publicity. There was tremendous publicity. Multiple documentary films were made. Books were written about the exploits – including one by Forbes Technology lead reporter, Parmy Olson. Matthew contributed his Internet Feds logs for her book.[33]

Insight into this zeitgeist is found in Janet Maslin's review of Olson's book for the New York Times:

> A lively, startling book that reads as 'The Social Network' for group hackers. As in that Facebook film the technological innovations created by a few people snowball wildly beyond expectation, until they have mass effect. But the human element - the mix of glee, malevolence, randomness, megalomania and just plain mischief that helped spawn these changes - is what Ms. Olson explores best...We Are Anonymous also captures the broad spectrum of reasons that Anonymous and LulzSec attracted followers.[34]

Lulzsec Sentences Compared to Keys' PSR Guideline Sentence[35]

---

[33] Parmy Olsen, "We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency."
[34] Janet Maslin "The Secret Lives of Dangerous Hackers: 'We Are Anonymous' by Parmy Olson." New York Times (May 31, 2012), available at http://www.nytimes.com/2012/06/01/books/we-are-anonymous-by-parmy-olson.html?_r=0.
[35] *See, e.g.*, "LulzSec Hackers Handed Down Prison Terms, Suspended Sentence, In Britian." RT (May 16, 2013), available at https://www.rt.com/news/lulzsec-sentence-jail-davis-376/.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Lulzsec or "Lulz Security" were a small offshoot of Anonymous that gained their heights of fame in 2011 for "hacking the planet," as the Internet community puts it. There were a series of high profile cyber-attacks carried out by Lulzsec beginning in May 2011. Targets included Sony Pictures' internal database, the CIA's website, the FBI's contractor InfraGard, the British equivalent of the FBI, "SOCA," the Westboro Baptist Church, Frontline, Fox News, and several of Rupert Murdoch's properties. Although the group officially announced its retirement in June 2011 they reunited to hack Murdoch's "Sun" newspaper in July 2011. Members of LulzSec included "Topiary" and "Palladium." The Sun front page was defaced to show a photoshopped prone Murdoch, who had suddenly passed away in his topiary from a lethal dose of Palladium. Nonetheless, Matthew faces a much harsher sentence than those meted out to Lulzsec. All the members of LulzSec/Internet Feds combined received sentences in the aggregate that barely exceeded the recommended sentence in this sentence. Comparatively, Keys' PSR guideline sentence of 87-108 months is excessive and disparate.

LulzSec periodically released stolen information from websites. They posted the stolen data on their website in .txt files, on the web app pastebin aka pastebin.com, in torrents on their page, or in downloadable files on the BitTorrent website the Pirate Bay. Releases often were posted on Fridays and thus they made a hash tag called "#fuckfbifriday" that they use to tweet with for their "fuck the FBI Fridays." LulzSec, like Internet Feds before them, used Distributed Denial of Service[36] actions and SQL injections[37] to take down websites. The group was motivated in part by political causes related to economic and social justice, but also seemed to appreciate hacking for pure entertainment. (See also: #OpSony)[38]

[36] This tactic, known as a DDoS, overwhelms a website with traffic such that it collapses under the weight of the DDoS. While it does no lasting harm to a website, it can knock a website offline for minutes, hours or days.

[37] SQL or sequel injections are incursions into a website after a vulnerability has been discovered. A sequel injection can lead to the compromise of an entire website. On multiple occasions, LulzSec used SQL injections to harvest databases and all of the contents of websites.

[38] Many news agencies incorrectly reported that LulzSec was responsible for the more damaging and headline-grabbing Sony Play Station intrusion. A few days before the Sony Pictures intrusion charged herein, Play Station was breached. A reported 77 million accounts were compromised. The damage was so extensive that Play Station was offline for approximately six weeks. See the website "Absolute Sownage" for a chart and explanation of the Sony hacks that surrounded this case. There were so many that a score sheet literally became necessary. http://attrition.org/security/rant/sony_aka_sownage.html

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

On May 5th, 2011, the earliest known hack attributed to Lulzsec began against Fox Broadcasting Company,[39] which resulted in the breach of TV talent show *X Factor* contestant's database and 73,000 applicants' personal information. On May 10th, FOX.com's sales database and users' personal information was released.

Between late May and early June 2011, international media company Sony's database was attacked by hackers who took thousands of users' personal data including "names, passwords, e-mail addresses, home addresses dates of birth." Lulzsec claimed that it used a SQL injection attack and was motivated by Sony's legal action against the original iPhone jailbreak hacker George Hotz, who revealed similar information of Sony's PlayStation 3 console in December 2010.

LulzSec breached databases include Sony Music Japan, Sony Pictures, SonyBMG Netherlands and SonyBMG Belgium. The group claimed to have compromised over 1,000,000 accounts, though Sony claims the real figure was around 37,500.[40] Some of the compromised information has been reportedly used in scams.[41]

On May 29th, 2011, LulzSec managed to compromise several PBS web properties including PBS's official website and Twitter account. The PBS homepage was defaced with an image of famous Internet meme Nyan Cat and the words "all your base are belong to lulzsec" referencing another Internet meme: All Your Base Are Belong To Us. Lulzsec claimed it was in response to a biased documentary about Wikileaks that had aired on an episode of PBS Frontline. They also were responsible for an article which claimed that 2Pac, a rapper who died back in 1996, was still alive and was found living in New Zealand with another famous dead rapper, Biggie Smalls.

LulzSec took responsibility for taking down the United States Central Intelligence Agency website in a tweet on June 15th, 2011.

On June 15th, 2011, an article was posted to the website VentureBeat claiming that LulzSec was starting to attack users of the website 4chan.org and Anonymous. The sparring began when LulzSec

---

[39] Internet Feds hacking activities began in December 2010, the time that Keys was in the chatroom.

[40] Keys' attorney Jay Leiderman represented one of the people charged in this SQL injection case. The true number is less than 37,000. Though there was over $600,000.00 in damage and personal credit information was posted publicly, Matthew faces over 7 times the punishment given out to the two defendants in Los Angeles.

[41] There was never any proof of this claim, and Leiderman was privy to the discovery in that case.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

initiated a "DDoS Party," which was a set of large-scale distributed denial of service attacks on several gaming servers and websites that brought a lot of games offline. EVE Online, League of Legends and Minecraft all faced outages or significant latency problems.

On June 19th, 2011, LulzSec posted a statement on the pastebin website announcing that they will be teaming up Anonymous to attack government agencies:

> Welcome to Operation Anti-Security (#AntiSec) – we encourage any vessel, large or small, to open fire on any government or agency that crosses their path. We fully endorse the flaunting of the word "AntiSec" on any government website defacement or physical graffiti art. We encourage you to spread the word of AntiSec far and wide, for it will be remembered. To increase efforts, we are now teaming up with the Anonymous collective and all affiliated battleships.

On June 20th, 2011, LulzSec managed to take down the United Kingdom's Serious Organized Crime Agency (SOCA) website with a DDoS attack as part of Operation Anti-Security.

On June 21st, 2011, a South American branch of Lulzsec group (@LulzSecBrazil) launched DDoS attacks against the portal of Brazilian government websites and the homepage of the President under the banner of Operation Anti-sec. The denial-of-service attacks came following the announcement on June 19th of a joint operation seeking to "steal and leak any classified government information, including email spools and documentation."[42]

From the onset of Operation Anti-sec, LulzSec's support base expanded from small unknown groups to an international network of Anonymous activists and regional Lulzsec chapters in Brazil and Colombia, as well as the Iranian Cyber Army.

On June 23rd, Lulzsec released a new set dubbed "Chinga La Migra," a Spanish phrase meaning "fuck the border patrol," which reveals hundreds of private intelligence bulletins, personal information of police officers and confidential documents including training manuals and personal email correspondence.[43] In the press release, the group cited the legislation of SB1070 (Support Our Law Enforcement and Safe Neighborhoods Act), a controversial anti-immigration law that was passed in the

[42] http://venturebeat.com/2011/06/22/lulzsec-brazil-hack-government/
[43] http://www.lataco.com/hacker-group-announces-chinga-la-migra-releases-classified-arizona-police-info/

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

state of Arizona in April 2011, as their primary motive behind targeting the Department of Public Safety.[44] The documents classified as "law enforcement sensitive", "not for public distribution", and "for official use only" are primarily related to border patrol and counter-terrorism operations and describe the use of informants to infiltrate various gangs, cartels, motorcycle clubs, Nazi groups, and protest movements.[45]

On June 25th, 2011, LulzSec released a statement on pastebin saying that after 50 days of hacking, they will be going into retirement. The farewell statements were accompanied by about 458 MB of data from AOL, AT&T, Navy.mil, pilimited.com, and many other websites that they uploaded from their Pirate Bay account.

On July 13th, 2011, LulzSec announced that once the @pastebin Twitter account reached 75,000 users they would embark on a mystery operation that would "cause mayhem." After their announcement, @pastebin received about 10,000 followers in 6 days.

On July 18th, 2011, the Lulzsec resumed its activities when they reportedly edited the *entire* homepage – the front page - of News International-owned *The Sun* to display a fake story about NewsCorp's CEO Rupert Murdoch's death from a drug overdose. As the volume of requests exploded on the news site, the group then redirected its homepage to their Twitter account. LulzSec also confirmed its responsibility for the hack and released a number of e-mails and passwords presumably associated with The Sun employees via Twitter. The tech blog Gizmodo also reported that one of the passwords tweeted out by "Anonymousabu" (Hector Monsegur) belongs to the arrested and now convicted (From the British phone hacking scandal) News International chief Rebekah Brooks: visited The Sun before we did this (may God have mercy on your soul) clear your cache so the redirect works. #MurdochMeltdownMonday.

"Both Sides of the Atlantic"

The Lulzsec members in England were charged under the U,K's Computer Misuse Act. The language of the Computer Misuse Act and the conduct it prohibits are similar to the CFAA. Indeed,

---

[44] Id.

[45] http://www.digitaltrends.com/computing/lulzsec-hits-arizona-police-computers-reveals-sensitive-data/

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

written in 1990, it appears Parliament reviewed the CFAA when drafting the Computer Misuse Act.[46] Accordingly, the crimes for which British Internet Feds/LulzSec members were convicted are analogous to the crimes that American participants of these groups committed. The sentences are thus relevant to determine a comparison between what actions and crimes were undertaken by these groups and how the punishments for those crimes would compare to a 87-108 month sentence meted out to Matthew for conduct that is, by comparison, *de minimus*. As the prosecution admits, "[t]his is not the crime of the century."[47] Yet he faces a far more severe sentence than any member of Lulzsec served. 60 months, which the Government seeks, would be more than any person engaged in hacking crimes during this period – by about double!

Sentence of Lulzsec Member Hector Xavier "Sabu" Monsegur: 7 months

The most active member and the identified leader of both Internet Feds and LulzSec was Hector Xavier Monsegur, who was in his mid to late 20's during his most active period. Monsegur is more famously known on the Internet as "Sabu." He is the same Sabu from the Internet Feds chatroom. After being arrested by the FBI in 2011, he cooperated heavily with the FBI and took a plea. In his plea he admitted participating in the Los Angeles time story prank.[48]

Indeed, in relation to Count 2 in his case, Sabu admitted to unlawful access of the Tribune Company's CMS, along with "attacks" on HBGary, a cyber security firm. In the HBGary hack, Sabu and Internet Feds co-conspirators appropriated and publicly released 70,000 emails. They infiltrated all parts of the company by "rooting" or gaining root access to all of HBGary's systems. The CEO of HBGary Federal, a division of HBGary, was fired. His personal iPhone, router, email, Twitter, Facebook, World of Warcraft and other accounts were appropriated. He also admitted to a hack of Fox's website, accessing the contestant list for the X-Factor TV show and releasing tens of thousands of contestant's information. The motivation for the hack was said to be that the CEO of HBGary Federal

---

[46] *Compare*, Computer Misuse Act 1990, available at http://www.legislation.gov.uk/ukpga/1990/18/contents, *with* 18 U.S.C. § 1030 (CFAA).

[47] Amul Kalia, "The Punishment Should Fit the Crime: Matthew Keys and the CFAA" Electronic Frontier Foundation, available at https://www.eff.org/deeplinks/2015/12/punishment-should-fit-crime-matthew-keys-and-cfaa.

[48] *See, e.g.* Anna Merlin, "Former Hacker Hector "Saabu" Monsegur Gets Time Served After "Extraordinary" Cooperation with Feds" Village Voice (May 28, 2014), available at http://www.villagevoice.com/news/former-hacker-hector-sabu-monsegur-gets-time-served-after-extraordinary-cooperation-with-feds-6718582.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

was going to meet with the FBI in an attempt to unmask members of Anonymous. This behavior relates to only count two of a twelve count complaint, and but one complaint of 4 across the country, including one in the Eastern District of California.

Sabu additionally admitted hacks unrelated to Anonymous or LulzSec where he stole from people's bank accounts. He also admitted to selling drugs. Furthermore, he admitted participation and leadership in the following hacks[49]: The Visa, MasterCard, PayPal and Amazon hacks called Operation Avenge Assange[50], attacks against the Tunisian Government in support of the Arab Spring uprising,[51] attacks against the Algerian government as part of the Arab Spring uprising, attacks against the Yemeni government, again as part of the Arab Spring uprising, attacks against the Zimbabwean government, and the later "dump" all the Zimbabwean data into the public sphere, Sony (multiple times including Sony Music, Sony Pictures and several foreign Sony companies), PBS, video game company Nintendo, the Georgia division of Infraguard (Infraguard is an FBI contractor), Unveillance (a cybersecurity company), the United States Senate (confidential information was downloaded and shared with the public),[52] video game company Bethesda Softworks, a hack of an automotive company in New York in which he, acting alone, was able to swindle the company out of 4 automobile engines worth approximately $3,500.00, fraud involving "dozens" of fraudulent or stolen credit cards upon which he personally made fraudulent charges, bank fraud committed upon the accounts of private citizens, and, finally, aggravated identity theft. The property crimes were not done in connection with Internet Feds or LulzSec.

Monsegur had 4 indictments total filed against him and dismissed in favor of the Southern District of New York plea. Monsegur pled guilty to 12 counts carrying with them a total maximum of 122 ½ years.[53] Additionally, "Monsegur also admitted to hacking thousands of computers between 1999

---

[49] *See generally*, *United States v. Hector Xavier Monsegur*, 11-CR-666 (LAP) (S.D.N.Y.), and exhibita 2 and 3.
[50] Operation Avenge Assange was mentioned in Matthew's trial and was discussed as a substantial motivating factor for Matthew wanting to report on, and joining Internet Feds. He was invited into the room by Sabu.
[51] This act was also occurring during Matthews' time in Internet Feds. Though not discussed at trial, this event was also very newsworthy and Matthew was attempting to get information about these politically motivated acts.
[52] Monsegur was not charged with the CIA or Britain's Serious Organized Crime Agency hacks.
[53] *See, e.g.*, Nate Anderson "Great Personal Danger: Inside Hacker Sabu's Guilty Plea Hearing" Arstechnica (May 9, 2012), available at http://arstechnica.com/tech-policy/2012/03/great-personal-danger-inside-hacker-sabus-guilty-plea-hearing/.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

and 2004, engaging in various hacktivism activities as well as carding activity — stealing and selling credit card information for financial gain or to pay off his own bills. He also admitting to selling a controlled substance, illegally possessing an unlicensed firearm, and purchasing stolen electronics and jewelry."[54]

Monsegur only served 7 months because of violation s of his supervised release including picking up a new charge (impersonating an FBI agent). He also violated his computer restrictions. But at sentencing he was given only 7 months with credit for 7 months served for violating the terms of his release.

Sentences for Lulzsec Members Darryn "PwnSauce" Martyn aka and Donncha "Palladium" O'Cerbagill: A $5,000.00 Euro Fine and a "Restorative Justice" class.

Lulzsec members Darryn Martin and Donncha O'Cerbagill were college students in Ireland at the time of their offenses. They were both around 19 years old. They pleaded guilty in July 2013 to criminal damage to the www.finegael2011.ie website. On January 9, 2011 the site was defaced, had its database stolen and was knocked offline for 24 hours - seven weeks before the general election.[55]

Both Martin and O'Cerbagill were also indicted in the Southern District of New York for computer crimes involving Internet Feds and LulzSec. Neither have been extradited, nor has extradition been sought for them or any of the members of Internet Feds and LulzSec that were indicted in the US but live in Britain.

Both Martin and O'Cerbagill are currently finishing up their college degrees.

Sentence for Ryan Ackroyd "Kayla" 30 months[56] of prison time.

Lulzsec member Ryan "Kayla" Ackroyd was co-defendants with fellow Lulzsec members Jake Davis, Mustafa Al-Bassam and Ryan Cleary in the U.K.'s prosecution for violations of the Computer Misuse Act. The British prosecution's sentencing summary listed some of the hacks Ackroyd, then 25, and his co-defendant's committed: The HBGary/HBGary Federal/Aaron Barr hack, Sony (multiple

---

[54] *See* Kim Zetter, "Government Seeks Seven-Month Sentence for LulzSec Leader 'Sabu,'" Wired (May 24, 2014), available at http://www.wired.com/2014/05/sabu-time-served-sentence/.

[55] *See, e.g.*, "Fine Gael website hackers spared jail sentences" RTE News (October 8, 2013), available at http://www.rte.ie/news/2013/1008/479105-fg-website-hackers-spared-jail-sentences/

[56] But See Jake Davis' statement: It was very[,] very unfortunate that Ryan Ackroyd did not wear a tag too for all of his police bail as he would have served considerably less. But the tag is highly disagreeable so I don't blame him one bit.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

times including Sony Online Entertainment, Sony Music, Sony Pictures and several foreign Sony companies, resulting in 12 days of outage time and a $20 Million loss), the Westboro Baptist Church (website defaced), video game company Nintendo, the Georgia division of Infraguard (Infraguard is an FBI contractor), Unveillance (a cybersecurity company), the United States Senate (confidential information was downloaded and shared with the public), video game company Bethesda Softworks, News International (Rupert Murdoch) "stable of websites," causing multiple high-profile news sites to go offline for hours[57] and for harvesting data from those companies, including the deface of the Sun in which Murdoch was declared dead, the Pentagon, wherein administrators were unable to access their accounts, causing 5 people to work for one month to remedy the problem, $100,000.00 in economic loss and $50,000.00 in new equipment needed to be purchased, 20th Century Fox's website, accessing the contestant list for the X-Factor TV show and releasing tens of thousands of contestants information, Eve Online, a gaming company, disrupting play for participants, SOCA, the British "Serious Organized Crimes Agency," the CIA, the British National Health Service, The Arizona State Police, which unleashed secret police data and information about the officers and ongoing investigations, along with information about police informants, and this is not an exhaustive list.. Mustafa recently was invited to 10 Dowing Street, home of the British Prime Minister, as part of a organization that is a "network of most promising entrepreneurial talent in technology."[58]

Ackroyd was trained on computers during his time in the British Army. He had previously participated in hacking groups that downed other targets, most notably "gn0sis." He had a virtual machine, and set up his equipment such that it would disable itself if a wire was touched. He was home when he was raided and tripped the wire himself. Scotland Yard was able to remove enough data from his virtual machine's memory to point clearly to Ackroyd's identity as "Kayla." "Kayla" was an assumed identity of a 16 year old girl. It was effective in throwing people off his trail.

Additionally, many of LulzSec's targets were taken out by Ryan Cleary (ViraL)'s use of a botnet. A botnet (also known as a zombie army) is a number of Internet computers that, although their

[57] In contrast to Keys, who never downed a network, but, rather, was convicted of aiding in a 40 minute edit of a minor article.

[58] Mustafa Al-Bassam, Twitter Feed (6:22am Mar. 4, 2016), available at https://twitter.com/musalbas/status/705715136393297920.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. A botnet is typically acquired by installing a "Trojan Horse" or "Trojan" on someone else's computer. The most common way this is done is to send an email and have the recipient click on a link or open an attachment. Cleary's botnet allegedly included 100,000 computers and was used to DDoS sites. It literally turned websites into smoking craters in cyberspace within seconds. This botnet was used on SOCA and the CIA, among other targets.

Ackroyd was sentenced to 30 months in prison. Ackroyd received a higher sentence than his co-defendants because he declined to wear an ankle monitor while on police bail (our equivalent of O.R.). Had he done so, his sentence would have been greatly reduced. British prison time is served at 50% if the prisoner is on good behavior. Additionally, Ackroyd was older and was a senior member of LulzSec, second only to Monsegur, and was considered Monsegur's 'Lieutenant." He personally found most of the vulnerabilities in the websites attacked. He was trained by the army and was presumed to know better than to use his skills in this manner.

Acroyd and Keys fought in the Internet Feds chatroom, ultimately leading to Keys' expulsion from the room. Keys was accused by many in the room of providing information to the media, thus violating the trust and security of the group.

Sentence for Jake Davis "Topiary" – 24 Months (half on probation)

LulzSec member Jake Davis was sentenced to a total of 24 months in the U.K., with 50% to serve in prison and 50% on probation. Electronic tag time knocked off all but 38 days of the first 50% prison time, hence 38 days remaining in prison, followed by 365 days on probation.[59]

Davis was not a participant of Internet Feds at the time Matthew was in the chat room. Davis's involvement began with the HBGary hack in February 2011. Davis was also convicted of all LulzSec Counts (aside from Monsegur no one in Internet Feds/LulzSec was involved in the conduct for which Keys was convicted). His computer had storage on it that included close to a million people's personal information. None of that information had been released to the public.

[59] Email from Jake Davis to Jay Leiderman.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Davis was responsible for LulzSec's witty antics on Twitter and elsewhere. He was the so-called spokesman for Internet Feds / LulzSec. He wrote the press releases for all of the operations and was the public voice of LulzSec. He is now a student studying theater. Davis is doing very well in school and his future looks rather bright.

Sentences for Mustafa Al-Bassam "T-Flow" "Chronom" (Internet Feds) –2 years suspended sentence.

Lulzsec member Mustafa Al-Bassam was a brilliant young coder who was an integral part of Internet Feds and LulzSec. He was present for all of the LulzSec crimes. Al-Bassam's crimes are almost identical to those of Ackroyd.

Matthew and Al-Bassam started to get along poorly in the Internet Feds' chatroom. Along with "Kayla," "Chronom" was a big reason that Keys' access to the room was revoked.

Al-Bassam is now a student at a London University. Like Davis, he is doing very well in school and his future looks bright.

Because Al-Bassam was a minor at the time of his arrest, details of the events that led to his arrest were never released.

Lulzsec Member Ryan Cleary "ViraL" [LulzSsec botnet herder]-32 months for 2 separate cases

Ryan "ViraL" Cleary was with LulzSec for only a short while, but his emergence marked their most "destructive" period. He was responsible for being the "bot herder"[60] that took down the SOCA and CIA sites. He was also said to be behind the U.S. Senate hack. Cleary was between 19 and 20 years old during the relevant periods.

Cleary rented his botnet out for cash. He allowed anyone to use it for any reason. Indeed, he had brokers taking a cut of the fee to help him keep it rented out. He had access to certain information involving true names behind XMPP[61] handles and IP addresses for those that put up text on Pastebin.com. Cleary used that information to cause negative consequences to people. For example,

[60] One who wields a botnet.

[61] Extensible Messaging and Presence Protocol (XMPP) is a communications protocol, much like IRC. People can chat privately or securely or small groups can have chats. People use handles in XMPP that look like email addresses, as opposed to IRC, where just the handle itself is used. For example, if AESCracked wanted to use XMPP he or she may choose AESCracked@jabber.ccc.de. Or AESCracked@duck.go or any other extension compatible with XMPP.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

when someone ran afoul of LulzSec, he gave personal information to Monsegur. The person's home was raided and his personal identity as well as all identifying information was made public.

He was arrested shortly after the SOCA and CIA attacks. Cleary did surprisingly little to hide his identity. He was released on his own recognizance and sent back home. He was rearrested later in 2011 for contacting Monsegur, then an FBI informant and asking Monsegur to help rehabilitate his reputation. As Cleary made it clear that he intended to use his reputation online again, he was remanded into custody before doing any damage.

Cleary was also found with locked portions of his hard drive. Based upon searches of his browser history, police believed him to be in possession of child pornography. They were unable to unlock his encrypted files. Eventually, faced with the threat of significant prison time, Cleary decrypted the files. It was never made public whether unlawful images were located.

It was also revealed that Cleary was involved in many other types of hacking activities and other unlawful conduct on the internet not involving his botnet. For example, he had been buying narcotic pills online. Much of Cleary's internet criminality was driven by his hatred of other Internet denizens.

Based upon the illegal pornographic images and the deadly botnet, along with Cleary's other aggravating conduct, Cleary was sentenced to 30 months. He and Ackroyd received the harshest sentences – though they were well less than half of what is proposed for Matthew.[62] This transcends the colloquialism "it hardly seems fair."

Reports are that Cleary has grown up a lot since this incident, or at least he is trying. He has asked his co-defendants, who are all doing well, for help getting his life on track. One week prior to his arrest, Cleary was diagnosed with Asperger's disease. He had been living in his room as a recluse for years. He did not attend school. He was on his computer all day and night. His windows were even covered with tinfoil.

[62] Reports from the time of sentencing: Cleary, 21, who also pleaded guilty to possession of images showing child abuse, was sentenced to 32 months, of which he will serve half. He also pleaded guilty to hacking and multiple counts of launching cyber-attacks against organizations, including the CIA and the UK's Serious Organized Crime Agency (SOCA), as well as hacking into US Air Force computers at the Pentagon; *see generally*, "LulzSec hackers handed down prison terms, suspended sentence in Britain" (May 16, 2013) Russia Today, (May 16, 2013), available at http://rt.com/news/lulzsec-sentence-jail-davis-376/; Susan Watts "Former Lulzsec hacker Jake Davis on his motivations" BBC News (May 16, 2013), available at http://www.bbc.co.uk/news/technology-22526021.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

He has since started making strides to a better existence. It will not be easy for Cleary, but he is seeking help. As with all of the other LulzSec and Anonymous defendants, he has rejoined society in a positive way.

No Charges for George David Sharpe aka "Sharpie"

George David "Sharpie". Sharpie was the individual who actually accessed the Tribune Companies CMS and caused the damage Matthew was convicted for. Sharpe was never charged on either side of the Atlantic. He was visited once at his home in Scotland by the FBI and Scotland Yard. He spoke to them and that was the last of his contact with this case.

The PayPal 14

The original "Operation Payback," discussed herein and at Keys' trial was an Anonymous operation that sought to counter a DDoS campaign by an Indian company who was said to have been hired by the "Bollywood" companies who were displeased with sites that did not take down copyrighted material quickly enough for their tastes. The company hired by "Bollywood" launched sustained DDoS traffic against many different sites, including the torrent website the Pirate Bay, because the Pirate Bay allows some users to download copyrighted material. That "Op" began in September 2010. Foreign companies continued to DDoS the Pirate Bay other sites and Anons[63] continued to counter-attack companies including law firms, the Recording Industry of America, and other pro-copyright sites. Op Payback lasted all the way until mid-December 2010.

In early December 2010, a banking blockade was formed with the intent that no donations were to be processed for the WikiLeaks "truth-telling" or "whistleblower" site. Op Payback quickly morphed into an action against donation payment processors PayPal, Visa, MasterCard and Amazon. Most people still called the DDoS protests against the banking blockade "Op Payback" but the operation was actually truly named "Op Avenge Assange," though so-called by few. These terms were used interchangeably throughout Matthews' trial, but were often just referenced as actions involving WikiLeaks or Assange.

[63] The colloquialism for those that self-identify as members of Anonymous

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Operation Payback members used a modified version of the Low Orbit Ion Cannon (LOIC) tool to execute the DDoS attacks. The LOIC operates by targeting a particular website with "junk" traffic.[64] The user types the site's URL into a bar on the LOIC and then clicks the "imma chargin mah lazer" button.[65] Junk packets are then sent to the target site. The net effect is that a website essentially refreshes itself over and over. By itself, the LOIC traffic is like throwing a pebble at a plate glass window. It is almost certain to do no damage. In September 2010, a "Hive Mind"[66] mode was added to the LOIC. While in Hive Mind mode, the LOIC connects to an Internet Relay Chat room, where it can be controlled remotely. This allows computers with LOIC installed on them to behave as if they were a part of a botnet. Utilizing this tool, the coordinators of Operation Payback were able to quickly take down websites belonging to anti-piracy groups. While tossing one pebble at a plate glass window may do nothing, tossing between 8,000 and 30,000[67] at once will likely have effect.

In January 2011, 40 warrants were executed in America in relation to the PayPal DDoS. In July, charges were filed against 14 people under the CFAA for their roles in the PayPal DDoS protest. It is estimated that between 8,000 and 30,000 people took place in the PayPal protest.

The PayPal defendants pled guilty to one felony CFAA count. They were placed on supervised release for one year with only one condition – do not commit any new crimes.[68] After a year, they were allowed to withdraw their felony plea. Misdemeanor pleas were entered. One or two of the defendants did not want to be placed on supervised release for a year, in that they had other criminal cases pending in State Courts in different jurisdictions, so they asked to be sentenced to 90 days in jail for an immediate misdemeanor. This plea was accepted by the District Court Judge in the Northern District of

---

[64] When one clicks on a link, a website is typically being asked to engage in a "handshake" with the requesting site. Then the requesting site may access the content of the linked site. Junk packets seek no handshake, they just cause the website's attention to be turned toward nothing of import.

[65] The tech staff at the Tribune Company at one point created their own DDoS tool called "bees with machine guns" that functioned in the exact same way as LOIC. Not only did they create it, they released it publicly with reckless abandon and even an acknowledgement that it could be used for illicit activities. (*See* "Bees with machine guns! Low-cost, distributed load-testing using EC2" Chicago Tribune, New Apps Blog, available at http://blog.apps.chicagotribune.com/2010/07/08/bees-with-machine-guns/.

[66] Many Anonymous chat logs during this period have the refrain "you have angered the hive."

[67] The estimated number of participants in the PayPal DDoSings.

[68] *See, e.g.*, Ryan J. Reilly "PayPal 14 Plea Deal Lets Hacktivists Avoid Felonies, Which is Pretty Much the Best They Could Hope For" The Huffington Post (Dec. 5, 2013), available at http://www.huffingtonpost.com/2013/12/05/paypal-14-plea-deal_n_4392521.html.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

California. Other than that, no one did a day in jail for a 4 day DDoS on PayPal that caused the world's largest online payment processor repeated outages during the holiday gift buying season. PayPal listed their damages at $5.6 million. The ultimate restitution figure settled on by the parties was just under $90,000.00, joint and several.[69]

The members of the PayPal 14 that have remained in the public sphere all are doing well, and have mostly gone back to their lives as they were before.

Vincent Kershaw, after sentencing but while still on the one-year probation, bought his first house in Colorado. He has stayed in the family landscape design/install business which he will be taking over later this year when his father retires.

Mercedes Haefer is working for an IT repair/service company in Las Vegas, continuing her studies at UNLV and, according to one of her co-defendants "basically being awesome."

Keith Downey roamed Europe looking for work for a few months but was unfortunately unlucky and didn't find employment. He moved back to Florida and is working at a hardware store saving money to get back to Europe.

Unfortunately, PayPal 14 defendant Dennis Collins, described below in the Payback 13 prosecution, has passed away.

The original Operation Payback and PayPal (Avenge Assange) in England, 4 more defendants

According to his court conviction after a trial in England, Christopher "nerdo" Weatherhead played a large role in Operation Payback (aka Operation Avenge Assange), described above. According to news reports, Weatherhead reportedly was instrumental in bringing down PayPal, resulting in £3.5million[70] in losses for the company. Weatherhead reportedly ran the AnonOps server. News reports alleged that some of the harmful packets that were sent to PayPal and others travelled through the servers he owned and operated. Per Weatherhead, it is not true that any harmful traffic travelled his servers, and this was not among the allegations levelled at him in his trial. If these news reports were correct, one would assume he would have been accused of those actions during his trial.

[69] According to Christopher Weatherhead, discussed below in the British PayPal prosecutions, "$4.2 million was consultancy fees, $185,000 was operational losses of the $5.6 million quoted by PayPal."

[70] This tracks with the $5.6M figure PayPal provided in the US case.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

In January 2013, Weatherhead was sentenced to 18 months in prison for his part in the denial-of-service attacks on PayPal, Visa and MasterCard in December 2010, as well as attacks on music, movie and other pro-copyright websites.

Also sentenced by the same English judge was Ashley Rhodes, 28. Rhodes was sentenced to seven months in prison for his role. A third man, Peter Gibson, 24, was given a suspended six-month prison sentence for his part in the Anonymous operations. The sentencing of a fourth man, Jake Burchall, 18, was adjourned.

The four men were each convicted of attacking anti-piracy and financial companies between August 2010[71] and January 2011. "Prosecuting, Joel Smith, said the four men were "not simply involved in the attacks, but played roles in maintaining the infrastructure used by other Anonymous members to coordinate attacks"."[72]

Weatherhead was described during his trial as a high-ranking member of Anonymous who owned two servers, ran private chat rooms and acted as a press spokesman to the world's media, including the BBC and Al Jazeera. The court heard that Weatherhead enjoyed such seniority that he held an election of Anonymous members to decide who or what would be the hackers' next target.[73]

Weatherhead is gainfully employed and had no issues with the law since being released from prison.

Payback 13

2 years after the PayPal 14 case first came to court, and after the re-pleader plea agreement was reached, the DOJ filed charges against 13 individuals in connection with the Visa and MasterCard DDoS protests in the Eastern District of Virginia. Pleas of 24-months prison time per defendant were offered to all 13 defendants. When the Judge Liam O'Grady was advised of the proposed pleas he erupted in anger at the government, demanding to know why the same crime would not be similarly punished as

[71] It appears that news reports might have that fact wrong, as all evidence points to the Anonymous activity beginning on September 21, 2010.

[72] *See* Josh Holiday "Anonymous hackers jailed for cyber attacks" The Guardian (Jan. 24, 2013), available at http://www.theguardian.com/technology/2013/jan/24/anonymous-hackers-jailed-cyber-attacks.

[73] *Id*.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

those in the Paypal 14 prosecution.[74] Weeks later, all 13 "Payback" defendants had pled guilty to a felony. The plea included a provision that after a year of supervised release wherein the only term was to not commit any new offenses, the felony plea would be withdrawn and a misdemeanor substituted therefor. The damage in that case was reportedly $8,917,010.82.[75] No one went to prison in that case.

Adam Bennett aka "Lorax"; Anonymous Australia Website Hacks, November 5, 2012

Over in Australia, Adam John Bennett, 42, who went by the handle "Lorax" was given a two year suspended sentence earlier this month (March 3, 2016) for six charges including aiding another person to cause the unauthorized impairment of electronic communications. In his case he admitted to charges that there were plans for a "mass defacement" of sites planned to mark Guy Fawkes' Day in 2012.[76] At sentencing the court was told Bennett helped an Australian juvenile dubbed 'Juzzy' to hack into a variety of sites, including those operated by the Australian Agency for Education and Training, the Australian Film Institute, Anchor Foods, and the Food Industries Association of Queensland. When the public tried to access a hacked sites, they found a message from the group in red text on a black background.

Prosecutor Patricia Aloi told the court "the plan was to get a much larger number of sites". She said the "impact could be described as a nuisance, could be described as lost productivity", and such offending could escalate.[77]

Bennett will end up doing 200 hours of community service for his juvenile nuisance behavior. The case in Australian bears many similarities to that of the instant case. This is especially so in light of the fact that "[Count 6] involved the website of Bennett's employer Cancer Support WA and that of HotCopper." Bennett tested the sites for vulnerability to the Heartbleed security bug, and tried to access confidential information.

---

[74] *See, e.g.*, "Felony charges? Harsh! Alleged Anon hackers lead guilty to misdemeanours" The Register (Aug. 20, 2014), available at http://www.theregister.co.uk/2014/08/20/anonymous_hackers_guilty_misdemeanours/; Attorney Leiderman has confirmed this with attendants of the hearing.

[75] *See, e.g.*, "Payback 13: Last of Anonymous anti-copyright hacktivists sentenced in Virginia" RT (Feb. 20, 2015), available at https://www.rt.com/usa/234191-anonymous-payback-collins-blake/.

[76] Guy Fawkes Day, November 5th, is a day celebrated by Anonymous as sort-of "their holiday." Many "ops" are set for the 5th of November. The date stems less from British traitor Fawkes himself, but rather from the movie ""V" for Vendetta."

[77] *See* "Former Anonymous member Adam John Bennett given suspended sentence for website hacking" ABC News Australia (Mar. 3, 2016), available at http://www.abc.net.au/news/2016-03-03/accused-hacker-adam-john-bennett-suspended-sentence/7217466

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Like the members of Internet Feds/LulzSec, minus Monsegur, Bennett is a high-profile and quite beloved member of Anonymous. He hosts a very popular talk "Lorax Live" show on AnonOps Radio.

Jonathan Cowden; Op Free Palestine

Jonathan Cowden, 27, was convicted in Federal Court in St. Louis, MO in 2013 for using online tools to attack Nefesh B'Nefesh, an Israeli organization started by and named for an Israeli rapper that assists immigrants to that country, between November 2011 and Jan. 17, 2012, and of hacking the Mayor of St. Louis. Cowden admitted he stole data, damaged computers and boasted about his exploits on Twitter as "_AnonymouSTL_" and elsewhere. Cowden worked for a company that advertises its ability to keep companies' online data safe. In at least one online profile, he bills himself as a "White Hat" hacker, someone who helps organizations identify security vulnerabilities.[78]

Cowden, for all of his various hacking activities detailed below, was sentenced to serve 15 months in a Federal prison and pay $22,000.000 in restitution. He gave an interview to Anonymous prison support network FreeAnons[79]:

> **Question**: Hi Jon, can you tell us about your case that resulted in your arrest and incarceration? Was your arrest related to OpPalestine?
> **Answer**: I was arrested and charged with one count of Computer Fraud – Access to a protected Computer causing $5,000 or more in damage. I plead to two infractions under that statute. One was for the attack on Nefesh B' Nefesh and one was for hacking Mayor Francis Slay. Nefesh B'Nefesh was part of a "fire sale" hacking campaign that I, myself completed against the Nation State of Israel. I also hacked TopLinks (Major News and Marketing),The Bar-Ilan University's Geography and Environment Department (Land, Oil, Diamonds and GPS) The Israel Institute of Technology: Techinon and their Cancer and Vascular Biology Research Center (Technology and Health ILAN (Charity Foundation – PsyOps) and SNIP (more news). What was not mentioned was that I also hacked SALT.IL (their LARGEST export) as well as the Israeli site of ARCO Oil. (Another of the TOP exports.) So you can see… I attacked LAND (GPS, Geology), Exports (SALT and Oil), Technology (Institute of Tech), Struck Fear (Charity) and took down News (Toplinks and SNIP).

[78] Robert Patrick "Feds say St. Louis man hacked Israeli group's data" St. Louis Post-Dispatch (Feb. 1, 2013), available at http://www.stltoday.com/news/local/crime-and-courts/feds-say-st-louis-man-hacked-israeli-group-s-data/article_f220d5ab-8b8e-5d50-b87b-3fb63d7465c9.html

[79] Freeanons, "Welcome Home Jon Cowden: Life after Prison #OpPalestine " *Freeanons.org* (November 3, 2014), available at https://freeanons.org/welcome-home-jon-cowden-aka-_anonymousstl_-life-prison/

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

> My hacking was not related to OpFreePalestine. As you trace back on Hackmageddon I WAS OpFreePalestine in the beginning.
>
> ***
>
> The hack on Mayor Slay of St. Louis was to demand the control of his officers during the eviction of the Occupy camp after the Occupy camps of Oakland, LA, and NY all went south. Being that St. Louis officers are notorious for brutality [ ] I felt it was required of me. It worked… Only a handful were peacefully arrested and released that night.

Cowden got 15 months, yet Matthew's guideline range is between 70 and 87 months and his PSR states that no *Booker* variance is appropriate. This interview should cause the Court to reject the guidelines entirely and start thinking about what type of *Booker* variance is appropriate. The comparative analysis of like cases shows that Keys' conduct was *de minimus*.

Cowden violated the terms of his supervised release by having an internet-accessible tablet and a pocket knife.[80] He was returned to custody. As one newspaper put it: "Jon explained to us at one point that even McDonalds wouldn't hire him because they use computers and they would have to be monitored. His self-confidence was squashed in prison and he suffered PTSD also as a result of his incarceration. [Cowden had many mental health issues prior to entering prison, and is now participating in counselling][81] Jon was beginning to feel better about himself. With the help of his beloved dog Chazz, an incredibly supportive girlfriend and a job in the works, life was finally looking up for our Anon that the world had forgotten.[82] All of that came to an abrupt halt on 10/25/2015 when Jon was arrested for violation of probation for being in possession of a pocket knife and a tablet computer.

---

[80] Per an email from Cowden's girlfriend: "With respect to recidivism (not sure if this helps your case or not) his only actual violation was that the pocket knife that was in my office (we weren't dating at the time - I'd set up an air mattress in there for him while he needed a place to stay) was slightly over the maximum length. He was allowed to have internet accessible devices (and he was allowed internet access) - he just had to have some spyware on whatever devices he used to access the Internet." The spyware to which she was referring was the monitoring software used by Supervised Release. He failed to inform supervised release of his new device.

[81] Per the same email: "So plenty of non-Anonymous factors that would have made him more likely to re-offend/differentiate himself from Keys." See note 85 as support of this claim.

[82] Cowden is known as the "Forgotten Anon" because his case received so little publicity in the Anon community. Through the work of FreeAnons, people have come to know who he is. As stated in an email by his girlfriend: "And for what it's worth, Jon's been dubbed "The Forgotten Anon" because no one knew about his initial arrest & incarceration until after he was released. So the only recidivist happens to be the only one who didn't have any support or contact with Anonymous from his arrest until after his release." Though Keys has no Anonymous support, the journalism community has been there for him, as has his amazing grandmother. His support network, primarily, is his work. He has always been there for journalism, and it has always been there for him.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Monsegur and Cleary violated terms of their pre-trial releases. Cowden is the only one that has violated terms of his supervised release and been returned to custody. It is rather noteworthy that everyone involved with Anonymous-related computer crime has returned to a happy and productive life. The recidivism rates among non-Anons and Anons are widely disparate. Recidivism rates in California are 61%.[83] Anons are, thus far, one out of dozens. That Keys has every prospect of living a crime-free, law-abiding life militates toward a conclusion that it is unnecessary to imprison him for any period of time. Keys' contrast with Cowden is among the starkest of contrasts that we will see in this comparative section.

Other instances of digital intrusions on Tribune Company

The alleged computer intrusion of December 2010 involving the LA Times compares with another type of intrusion that struck the Tribune Company more than 20 years earlier.

On November 22, 1987, the broadcast signal of Tribune-owned WGN-TV was briefly interrupted during a late evening newscast when a video pirate hijacked the signal to air videotape of a satirical parody involving a well-known television character known as Max Headroom.

According to engineers at WGN-TV as retold by the Chicago Tribune, an unidentified individual overpowered the television station's broadcast signal — likely through the use of sophisticated transmission equipment and technical knowledge of radio frequencies — gaining brief control of WGN-TV's airwaves. The intruder replaced WGN-TV's signal with his own, airing a videotape of someone dressed in a Max Headroom costume for about 30 seconds before WGN-TV's engineers were able to retain control of their airwaves. More precisely, during highlights from the Chicago Bears' 30–10 home victory over the Detroit Lions that afternoon in the sports report, the screen went black for 15 seconds, then returned with a person wearing a Max Headroom mask and sunglasses, moving around and jumping. His head was in front of a sheet of moving corrugated metal, which imitated the background effect used in the Max Headroom TV and movie appearances. There was no audio other than a buzzing noise and an oscillating sound.

[83] Department of Corrections And Rehabilitation - State of California, "2013 Outcome Evaluation Report" *Office of Research* (January, 2014), available at http://www.cdcr.ca.gov/Adult_Research_Branch/Research_Documents/ARB_FY_0809_Recidivism_Report_02.10.14.pdf

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

The incident left sports anchor Dan Roan bemused, saying, "Well, if you're wondering what's happened, so am I." He then unsuccessfully tried to repeat what he was saying before the incident occurred, having succumbed to laughter.[84]

The Max Headroom incident made national headlines and was reported on the CBS Evening News the next day. Not long after the incident, WMAQ-TV humorously inserted clips of the hijacking into a newscast during Mark Giangreco's sports highlights. "A lot of people thought it was real – the pirate cutting into our broadcast. We got all kinds of calls about it," said Giangreco.[85]

A few hours after the WGN-TV signal intrusion, another signal hijacking occurred, this time on public broadcaster WTTW during the airing of an episode of "Doctor Who." This time, the individual was able to gain control of WTTW's airwaves for close to two minutes (WTTW would later acknowledge it had no engineers on staff at the time who were capable of overriding the pirate's signal). Because Doctor Who was a popular program at the time, a number of people had taped the episode involving the signal interruption; copies of the incident were made available to local news broadcasters in the days to come, and have been preserved in recent years on websites like YouTube.

The so-called "Max Headroom pirate incident" was dismissed by the Chicago Tribune newspaper as a "silly stunt involving a parody of a parody," and the alleged pirate was referred to as a "joker" with a "strange sense of humor." But the Federal Communications Commission, the federal agency in charge of regulating television broadcasts among other things, did not find it to be strange or humorous: An immediate investigation was launched to determine the source of the signal intrusion and to identify those responsible for it.[86]

The Max Headroom incident is still the subject of prankster-fueled comedy. The most famous usage of the incident is probably when parts of the video were included in some episodes of the

---

[84] *See* "WTTW Chicago - The Max Headroom Pirating Incident." YouTube. The Museum of Classic Chicago Television, 22 Nov. 1987. Web. 09 Mar. 2016. https://www.youtube.com/watch?v=cycVTXtm0U0 ; *see also* "Captain Midnight, HBO, 1986." YouTube. N.p., 27 Apr. 1986. Web. 09 Mar. 2016. <https://www.youtube.com/watch?v=lbruOe6Yii0> ; *see also* "ABC News Report on HBO's "Captain Midnight"" YouTube. ABC, Apr. 1986. Web. 09 Mar. 2016. https://www.youtube.com/watch?v=xcQHc1zASDw .

[85] I*d.*

[86] *See* "Dr. Who And The Electronic Pirate" Chicago Tribune (November 30, 1987), available at http://articles.chicagotribune.com/1987-11-30/news/8703300133_1_max-headroom-stunt-invader.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

animated talk show, Space Ghost Coast to Coast. One can see the bobbing figure of the Max Headroom intruder going by when Moltar, a character in the show who is a kind of assistant to the main character , is switching feeds to get Space Ghost, the talk show host, his next guest.[87]

Though these intrusions were then and are now seen as harmless pranks, broadcast signal intrusions — in many ways, a form of television "hacking" — can have serious consequences. Had a local, state or national emergency occurred at the time of the signal intrusion, the two broadcasters in question who were hijacked would likely not have been able to invoke the Emergency Broadcast System, which could have jeopardized the safety and security of their viewers. Additionally, because signal intrusions at the time required pirates to overpower a frequency with more radiative power, the possibility of damaging broadcast equipment in this case was very real (neither broadcaster, in this case, reported damage to their equipment and, in fact, continued broadcasting as normal after the signal intrusion). Unlike hijacking a TV signal, altering the content of one LA Times article did not render the rest of the website inaccessible, posed no immediate or future danger or threat to the public and did not — by the government's own admission — cause any lasting damage to the computer equipment used to operate the website or the website itself.

Although the Max Headroom pirates were never found, their punishments would have likely mirrored that of another signal pirate: One year earlier, satellite engineer John R. MacDougall briefly overpowered the broadcast signal of the Home Box Office (HBO) as protest to the network's decision to begin charging satellite customers for HBO by encryption what had otherwise been a freely-available channel to them.

The incident became known as the "Captain Midnight signal intrusion" because of MacDougall's use of the moniker Captain Midnight. MacDougall used his position as a broadcast engineer and his advanced technical skill of signals and frequencies to overpower HBO's broadcast in the evening of April 27, 1986, causing customers to lose access to HBO programming for a few seconds.[88]

MacDougall was arrested following a year-long FBI investigation. Despite the FBI and FCC's assertion at the time that broadcast signal intrusions were serious crimes that carried severe

[87] https://en.wikipedia.org/wiki/Max_Headroom_broadcast_signal_intrusion

[88] This illustrates a true use of a "special skill" within the meaning of the sentencing guidelines.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

consequences and threatened national security, MacDougall was sentenced to serve one year of probation and ordered to pay a $5,000 fine. In a phone interview 25 years after the signal intrusion, he offered no remorse for his actions, saying he did "not regret trying to get the message out to corporate America about unfair pricing and restrictive trade practices."[89]

These pranks, while potentially serious, highlight an important dichotomy. There is a difference in intent. Monsegur had malice in his heart when he stole engines and used citizen's credit cards. Though there were consequences to Tribune Co. from the intrusion in this case, it came at a time and place where pranks were the norm. The very essence of "Chippy 1337" is, at its heart, a joke. In contrast to the WGN signal intrusion, the LA Times edit would have been lost to history if the LA Times themselves did not print an article with a screen capture of the initial edit.

Attorney Jay Leiderman has surveyed every prosecution and sentence for a member of Anonymous globally that he could find.[90] None come near the recommended PSR sentence for Matthew. Besides this glaring fact, other factors argue for a downward departure from the guidelines range.

Keys did not believe the login credentials used to access the LA Times would work

While barely awake, Keys gave an interview to the FBI. He was under the influence of medication. Still, per the government he was able to accurately describe events. If that is so, it is important to note the following from the recorded interview as transcribed in the FBI's "302" report on the interrogation:

> John Cauthen (JC): "You were not a hacker, per se, but at the end of the day, you did take e-mails from FOX40 that you shouldn't have, OK? And screw with them and cause them consternation."
>
> Matthew Keys (MK): "Hey, I really didn't take —"
>
> JC: "Well, stop for a second." (continues)
>
> [later]

[89] Paul McNamara, "Captain Midnight: 'No regrets' about jamming HBO back in '86," *Networkworld* (April 26, 2011), available at http://www.networkworld.com/article/2229101/security/captain-midnight---no-regrets--about-jamming-hbo-back-in--86.html

[90] See the more extensive white paper, attached hereto as Exhibit 1.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

JC: "I don't know all of the details, so, we're going, I mean, what we'd like to do—"

MK: "I, unfortunately, don't remember all of the details."

JC: "We'll refresh your memory of what we know."

[later]

MK: "I…told him that I had credentials for their CMS…and he asked for them…and I gave them to him…um…"

JC: "Why did you do that?"

MK: "Because I thought they didn't work."

Use of a VPN (Overplay)

Matthew did have access to a VPN service, but he used that service primarily in his capacity as a journalist for FOX40. The program, called Overplay, was installed on at least two computers at FOX40, and may have been installed on other computers. The program was also, for a time, installed on Keys' home computer. As far as Matthew knows, the program was not removed from any of FOX40's computers upon his exit, and because the account remained active, it is reasonable to assume that someone at FOX40 could have accessed it in the way they accessed any other program on the computer.

This illustrated that Overplay was not used solely for nefarious purposes. There are many legitimate uses for a VPN, and the installation of Overplay at FOX40 shows legitimate use. Overplay was software Matthew used during the course of his employment at FOX40 in order to watch geoblocked news channels from other countries.

One thing that no one can dispute is that Matthew is a massive news junkie, and that he spends all day every day searching the four corners of the Earth to find and scoop a story.

Screen Shots

Per the Government's objections to the PSR: "Keys further admitted taking screenshots of Internet chats he wished to retain, and acknowledged participating in the chat referenced in the search warrant application."

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

This is part true. He did create screenshots of his observation of Anonymous from various online chat rooms, including "Internet Feds." He also accepted logs — including screen shots — taken by others as part of his research into the story. He also downloaded logs that had been made freely available on the Internet that referenced activity that he had not observed.[91] Some of these logs were accessible on an external hard drive that was seized by the FBI in October 2010; some of them were not kept after his story ended in 2011 and are presumed gone for good. However, the FBI has also produced logs and screenshots it claims he created and/or had on an external hard drive seized that he had not seen before, including logs that reference the criminal allegations against him.

Keys wrote stories or provided information to journalists about Internet Feds

Matthew, as a serious journalist, was in the Internet Feds chat room to gather information for a news story. His access to the upper echelon of Anonymous was unprecedented. The information he passed on to other news sites was valuable in helping the world understand who these mysterious politically-motivated pranksters were. Additionally, he provided information to Parmy Olson, a Forbes journalist, for her aforementioned book on Anonymous and LulzSec. His provision of this information is what initially brought the FBI to his door. As a journalist he declined to reveal his sources for whom he granted protection as a condition of receiving information for his reporting. Matthew has made plain in the press that he believes this is what made him a target for prosecution.[92]

For the PBS NewsHour, Matthew provided three pages of documents taken from a Pastebin.com file that circulated in the InternetFeds chatroom. On the Gawker.com story, Matthew provided background information — based on what he knew — about a computer intrusion involving Gawker's comment database, but he did not provide any logs or material documents to Gawker. For Reuters,

[91] A person named Laurelai Bailey logged a section of the chats in Internet Feds and released them publicly. "Bailey says Lulz Security hackers hold a grudge against her for leaking logs from the secret chat room in which they planned the HBGary hack—which she says she did in retaliation for them harassing some of her friends." http://www.wired.com/2011/06/lulzraid/

[92] *See* Hari Sreenivasan "Gawker Data Breach Could Lead to Attacks on Government Agencies" PBS NewsHour (Dec. 12, 2010), available at http://www.pbs.org/newshour/rundown/gawker-data-breach-could-lead-to-attacks-on-government-agencies/; John Cook and Adrian Chen "Inside Anonymous' Secret War Room" Gawker (Mar. 18, 2011), available at http://gawker.com/5783173/inside-anonymous-secret-war-room; Matthew Keys "The InternetFeds: Inside hacker Sabu's war room" Reuters (Mar. 7, 2012), available at http://webcache.googleusercontent.com/search?q=cache:THzn_4yj1b8J:blogs.reuters.com/matthew-keys/2012/03/07/the-internetfeds-inside-hacker-sabus-war-room/+&cd=1&hl=en&ct=clnk&gl=us&client=opera.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Matthew filed a story one day after it was announced that Monsegur and others had been arrested at the request of a Reuters editor. A second editor re-wrote the majority of the story; he appears uncredited.

FOX News is not related to FOX40 Sacramento

Matthew worked for FOX40, the Sacramento affiliate of Fox. As was explained at trial, it is not a Fox station. FOX40 used Fox programming that it purchased from FOX. It had local news and had no relation to Fox News. As we know, FOX40 was owned by Tribune Media Company.

It was stated at trial that Matthew said in Internet Feds: "[i]f you want to attack FOX News, pm me, I have a user [name and] password for their CMS."

But Matthew never worked for FOX News, and did not have access to their CMS, except for access to a video distribution system provided to affiliates that was only accessible on a special computer connected to an internal network.

Keys statement to the FBI accepts responsibility

During his interview with Agent Cauthen, Matthew explained why he wanted to talk with the FBI: "This is one of the reasons why I'm talking to you as opposed to saying, you know, I want a lawyer or I want to talk to, you know, counsel at Tribune or -- again, I'm sorry, counsel at Reuters -- or anything like that is because, you know, I did it."

The edited LA Times.com story was never unavailable in its original form

The contention has been made by the Government that: "Defendant fails to address the fact that when he conspired to alter the contents of the Los Angeles Times, the original, unaltered content was therefore unavailable to the newspaper's readers."

This is incorrect. Articles that appear on the Los Angeles Times website also, at that time, appeared in syndication on every Tribune website property. An alteration to an article on one website did not impair the ability to read the articles on other websites. In any case, articles that appear on the Los Angeles Times website also appear on non-Tribune websites (through the Tribune Wire Services), in print (both in the Los Angeles Times and other papers both owned and not owned by the Los Angeles Times) and elsewhere (on their phones, in apps, etc.) where the article would have presented in its original form. Unless users have a special internet connection that forces them to read Los Angeles

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Times stories on the Los Angeles Times website, they are free to access the same story elsewhere and in other forms.

AESCracked

Matthew told FBI agents that he had selected the moniker AESCracked in order to appear authentic or knowledgeable to hackers...and although he did not know what AES was, he knew that Anonymous would.

This is true. He did use "AESCracked" in some of his interactions with members of Anonymous, and especially in the Internet Feds chatroom. He also used various other nicknames. None of the nicknames were locked with a password, meaning they were freely available for anyone to use on that particular IRC network. For most public IRC networks, using a password with a nickname — "reserving" — is optional, and that was the case here; he did not set a password because he did not believe other people would use it, though other people were certainly free to use it if they wished. He later learned, because of this case, that employees at Tribune Company who had administrative access to all websites were also mingling among Anonymous members. The allegation is not that Tribune employees had anything to do with AESCracked, but simply that the monker was available for anyone who wished to use it.

FBI Agent John Cauthen

Based on trial testimony, FBI Agent John Cauthen attempted to contact Matthew at his apartment in Sacramento, then attempted to gain entry to the apartment and collect information on Matthew by visiting the leasing office. When that failed, Cauthen called Matthew while he was en route to his new home (coincidentally, Matthew was moving the day Cauthen came to his apartment, and the apartment was vacated by the time he arrived).

During the phone call, Cauthen advised Matthew he was conducting an investigation and was interested in speaking with him. When Matthew asked what the investigation was about, Cauthen said he could not say. When Matthew ventured a guess and asked if it was about recent news reports he had worked on concerning Anonymous, Cauthen again said he could not say.

During the call, Cauthen asked if Matthew would be able to meet with him in his office or at another location, whichever was convenient for Matthew. He asked if Matthew could bring his

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

computer for examination because Cauthen felt it might be able to assist with an active FBI investigation. When Matthew told him he would be unable to provide Cauthen any material concerning any reports for which Keys provided sources confidentiality, Matthew again asked if Keys would be willing to meet him with his computer.

At that point, Matthew told Cauthen he would have to end the phone call because he was driving, but that Keys would be happy to assist him if Matthew could provide some information about his investigation and so long as it did not involve violating journalistic ethics. A few hours later, KGO-TV contacted Matthew regarding an application of employment, and Keys forgot about Cauthen's call.

Cauthen e-mailed Matthew a few weeks later to ask about a home address and other contact information for Matthew. Matthew opened the e-mail while he was at work, and intended to respond when he got home, but forgot about the message.

In March 2012, the dat it was revealed that Hector Monsegur had been cooperating with the Government for the better part of a year, Matthew learned that six suspected members of Anonymous had been arrested, including some he recognized from Internet Feds. Some of the conduct alleged included an attack on a computer system based in Sacramento belonging to a government contractor. In an attempt to get more information as part of his job duties at Reuters, he e-mailed Cauthen from his work e-mail address to inquire about the arrests and investigation in Sacramento. Cauthen did not respond.

Cauthen was present when the search warrant was executed, and asked many of the questions during the 2.5 hour interview/interrogation of Matthew. Cauthen recorded portions of the interview, and did not record other portions, including a portion during which Cauthen shadowed Matthew as he made a written statement.

No criminality before or since

The acts for which Matthew was convicted stem from the end of 2010. This brief is dated March 9, 2016. 5½ years later. Matthew has no criminal record and is a criminal history category zero. In the interceding 5 ½ years Matthew has committed no crimes. He has appeared in this Court every time he was required to, complied with every order, and never violated the terms of his supervised release. This militates strongly toward the conclusion that Matthew needs no custodial sanction.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

The CFAA is flawed and punishments are disproportionate to the crimes themselves and the true harm caused; true, this is "Not the case of the century."

Based upon enhancement levels for loss, sentences for CFAA crimes that may otherwise seem *de minimus*, like this case, for example, are beset with guideline ranges that are grossly disproportionate to the actual crime itself. The crime, in that it leaves such unfettered discretion and carries such harsh penalties, has been referred to privately as the "Prosecutor's best friend".[93]

According to Digital rights group and the leading authority on cyber-law, the Electronic Frontier Foundation, commonly known as the EFF: "One of the basic tenets of a civilized society is that the punishment should be proportionate with the crime. What essentially amounts to vandalism should not result in even the remote possibility of a 25-year jail sentence. But that very possibility is on the table in the government's case against journalist Matthew Keys, whose sentencing hearing is about one month off. The case is an illustration of prosecutorial discretion run amok—and once again shows why reform of the federal anti-hacking statute, the Computer Fraud and Abuse Act (CFAA), is long overdue."[94]

The EFF op-ed piece goes on to state, as Assistant U.S. Attorney Matthew Segal put it:

> "This is not the crime of the century." But the government still charged Keys with three federal felony violations of the CFAA …. Keys was convicted … and faces a maximum punishment of 25 years in federal prison—10 years each for the first two offenses and 5 years for the third. This case underscores how computer crimes are prosecuted much more harshly than analogous crimes in the physical world."[95]
>
> "It's true that Matthew Keys' actual potential jail sentence could be significantly less than 25 years. The government has actually signaled—but not promised—that it will "likely" seek less than 5 years. And it's conventional wisdom that maximum punishments may sometimes be a ploy to capture the public's attention …. But as [the EFF has] explained before, the maximum punishment can impact calculations pursuant to the United States Sentencing Guidelines. For instance, many prosecutors and judges use the maximum punishment as an indicator of how serious the crime is. They also ratchet up pressure on defendants to plea bargain or

[93] *See, e.g.*, Kim Zetter "Hacker Lexicon: What is the Computer Fraud and Abuse Act?" Wired (Nov. 28, 2014), available at http://www.wired.com/2014/11/hacker-lexicon-computer-fraud-abuse-act/.
[94] Amul Kalia "The Punishment Should Fit the Crime: Matthew Keys and the CFAA" Electronic Frontier Foundation (Dec. 16, 2015), available at https://www.eff.org/deeplinks/2015/12/punishment-should-fit-crime-matthew-keys-and-cfaa.
[95] *Id.*

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

> settle—after all someone facing 25 years is more likely to agree to serve five than someone facing a maximum of five year penalty."[96]

Such is the case here. Matthew took not only a great risk, but a courageous stand in taking this case to trial. It is everyone's right to take a case to trial. It is a constitutional right to put the Government to their burden of proof. Matthew should not suffer additional consequences for putting the Government to task. If the Government believes this is a just law, that it is something they should stand behind, and they should be proud to take the case to trial and defend the law as written. Moreover, it is not logical to assume that one who takes a case to trial will, before an appeal is heard, will express an acceptance of responsibility. If the case is remanded for a new trial, Matthew would be stuck with his statements of remorse and contrition. He intends to appeal, and intends not to do anything to harm his chances on appeal.

To be sure, the Government will likely argue that his failure to plead guilty evinces a lack of an acceptance of responsibility. But in the face of an unjust, out of date law with punishments far exceeding the nature of the crime, it is the duty of conscientious Americans to challenge the law. One does so by taking the case to trial. This is hardly failing to accept responsibility; it is taking on a greater responsibility. It is sacrificing ones' self at the altar at liberty[97] to draw attention to a manifest injustice. THE CFAA seems to change with each appeal. Matthew's case should be no different. Whether his case helps him or not, it will help clarify a muddy, out of date law.

The CFAA was written in 1984, largely as a response to the movie "War Games." It was written when the internet was in its nascency. In 1984, one had to use a modem to dial up a particular computer network to access their information. To gain information from, for example, Stanford University, you had to seek out the University itself, dial it up like a telephone number, and access it, and only it. You were, in essence, going to a stand-alone store to shop.

In 1991, http protocol was invented. At that time, one could simply type Stanford.edu into a browser and – bingo – your computer was connected to Stanford University. HTTP protocol and browsers made the internet more akin to shopping at a mall, one could roam from store to store freely

---

[96] *Id.*

[97] See Andrew Auernheimer's speech as he's going to prison in "The Hacker Wars," a documentary on hactivists: https://www.youtube.com/watch?v=ku9edEKvGuY Matthew declined to be interviewed for the movie. Though Auernheimer is seen by many as less than a great individual, the quote is apropos.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

and conveniently. 1984 was a whole different world than March 2016, or even December 2010. Yet the harsh online civilization of 1984 is still being revisited in 2016 via the CFAA. Despite the wild variance in the types of crimes committed in 1984 and 2010, the elements of the crimes and the punishments remain the same. Again and again, computer criminals are treated like thought criminals and are sent off to the proverbial Room 101.

These inequitable penological results are a direct correlation to the fact that we are using horse and buggy laws to handle a jet plane society. On that fact alone Matthew deserves a *Booker* variance.

ARGUMENT

Mr. Keys requests custodial release for the following reasons:

1. The guidelines range calculations apply inappropriate conduct-based enhancements,
2. Mr. Keys did not employ "sophisticated means" in these offenses,
3. Mr. Keys did not exercise managerial or supervisory authority over any conspiracy,
4. The loss calculations in the PSR are contrary to sentencing law and policy,
5. Numerous factors under 18 U.S.C. § 3553(a) merit a downward departure from the guidelines range,
6. The Defendant's personal and professional history merit downward departures from the guidelines range,
7. A sentence under the guidelines range would not satisfy the traditional goals of a criminal sentence, and
8. A downward departure is necessary to prevent a disparity in sentences for similar or more serious offenses.

I. BASELINE GUIDELINES SENTENCE LEVEL

When imposing a sentence, a court should start by calculating the applicable Sentencing Guidelines range. *Gall v. United States*, 128 S. Ct. 586, 596 (2007). The base offense level for a conspiracy (18 U.S.C. § 371) to damage a protected computer (18 U.S.C. § 1030(a)(5)(A)) is 6.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

U.S.S.G. § 2B1.1(a)(2); see also *id.* § 2X1.1(a) (base offense level for conspiracy identical to base offense level for substantive offense). The loss, estimated in the PSR at $249,956 adds 10 levels. *Id.* § 2B1.1(b)(1)(F). The Guidelines add 2 levels each for obtaining/disseminating personal information and for use of special skills. *Id.* §§ 2B1.1(b)(16), 3B1.3. Mr. Keys alleged role in the conspiracy, a supervisor or manager of a conspiracy involving five or more participants, adds 3 levels. USSG § 3B1.1(b). There is no victim related enhancements, obstruction of justice, or acceptance of responsibility enhancements added to recommended sentence. (PSR at 8). The applicable offense level, therefore, totals 29. (PSR at 3). The offense level of 27, absent any prior criminal history, is accompanied by 70-87 months of imprisonment, 1-3 years of supervised release, and 1-5 years of probation. The probation office recommended penalties, however, that are on the lower end of the guidelines. The PSR only recommends 70 months of imprisonment, 2 years of supervised release, and no probation. (PSR at 3).

A. SOPHISTICATED MEANS

The PSR enhances Keys' sentencing on the basis that he "intentionally engaged in or caused the conduct constituting sophisticated means" under U.S.S.G. § 2B.1(b)(1). According to the PSR, the "sophisticated means" consisted of only these uses: 1) "fake email addresses;" 2) use of a proxy service; and 3) "enlist[ing] the services of highly skilled hackers." However, none of these is a sophisticated means within the meaning of the Sentencing Guidelines. In fact, the USSC amended the definition of "sophisticated means" to "narrow" (its own words) its scope to avoid precisely this kind of application. The PSR's conclusion is wrong because: 1) the USSC declined to include proxy servers in its definition of definition of "sophisticated means;" 2) the USSC narrowed the definition of sophisticated means to cases where the defendant "intentionally engaged" in the sophisticated means, so as to enhance based on the defendant's own culpability rather than the device used; 3) proxy servers are commonplace and widely used for predominantly legal and ethical purposes; and 4) the use of an alias in an email address is also a common practice and does not make it a "fake email address."

1. The USSC Decided Not to Include Use of Proxy Servers in its Definition of "Sophisticated Means"

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

To conclusively define Keys' use of a proxy server for his personal use as a "sophisticated means" is inconsistent with the USSC's intent, as they previously considered adding proxy servers to the definition, and declined to do so.

On March 17 and 18, 2009, the USSC held public hearings on proposed amendments to the Sentencing Guidelines, including a proposal to include use of a proxy service in connection with the charged offenses.[98] Specifically, the proposed language would read: "In a scheme involving computers, using any technology or software to conceal the identity or geographic location of the perpetrator ordinarily indicates sophisticated means."[99] Thus, had that language been introduced, the burden would have shifted away from the government merely because the defendant had used some kind of proxy service.

The USSC heard numerous speakers on the issue, including representatives from the Department of Justice, Identity Theft Resource Center, Federal Public and Commffakeunity Defenders, and the Electronic Frontier Foundation.[100] After considering the arguments, including those of its proponents, the USSC declined to add use of proxy server to the definition. The definition of "sophisticated means" has since been amended to narrow its scope (see below), but without this addition.

The reasons why the USSC decided not to include this addition are evident from the testimony before the USSC. Most people who use proxy servers do so for legitimate and ethical purposes. Many use them without knowing at all how they work, or even that they are using them at all. These services are installed, often by others, and many forget that they are even using one. As the Federal Defender testified, penalizing the use of a proxy "will absolutely sweep in conduct that is not especially complex or especially intricate," adding that the DOJ "would have us believe that any technology or software to hide identity or location meets that test, and it is simply not true."[101] Even the DOJ, when pressed,

---

[98] United States Sentencing Commission, Public Hearing, March 17 and 18, 2009, available at <http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-hearings-and-meetings/20090317/Transcript.pdf>.

[99] United States Sentencing Commission, Proposed 2009 amendment to Application Note for Sophisticated Means Enhancement under Subsection (b)(9), January 27, 2009, available at http://www.ussc.gov/sites/default/files/pdf/amendment-process/reader-friendly-amendments/20090127_RFP_Amendments.pdf.

[100] *Id.*

[101] United States Sentencing Commission, Public Hearing, pg. 36

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

acknowledged that use of proxies is not in of itself illegal, agreeing with the EFF that any use of a proxy service must be analyzed on a "case-by-case" basis.[102]

But the PSR concludes, without explanation, that the use of the proxy service alone requires an enhanced sentence, merely because the server itself was located in Switzerland. (PSR at 8). This is the overbroad conclusion that the USSC was asked to avoid, because it "would create a wholesale presumption in conflict with actual evidence" and "relieve the government of proving the purportedly aggravating fact in any given case and shift the burden to the defendant to prove that the enhancement should not be followed."[103] The conclusion ignores the fact that proxies are used for a wide variety of activity, much of which is not criminal, and generally do require any kind of technical sophistication.

For instance, Matthew used a VPN proxy server in his capacity as an employee at Fox40, with the knowledge and approval of Fox40's IT Manager, to follow international news feeds which might otherwise have been unavailable due to geographic blocking. Fox40 installed the software on Matthew's computer. Other employees used a VPN as well, because it is a valuable investigative and journalistic tool.

There is no evidence that Keys employed any sophistication with his use of a VPN. The VPN is merely a tool that had been installed on his computer, for investigative and privacy purposes. The presumption that its general use categorically requires enhanced sentencing was rejected by the USSC. Thus, the government's reliance on the proxy server as a sentencing factor is unsupported.

2. <u>Neither the PSR Nor the Government has Established that Keys "Intentionally Engaged" in the Sophisticated Means, as Required by the U.S.S.G.</u>

The USSC declined to amend the Sentencing Guidelines so broadly as to include proxy servers, and in fact amended the definition of sophisticated means to *narrow* its scope. Under the amendment, the guidelines clarify that the "defendant intentionally engaged in or caused the conduct constituting the sophisticated means." U.S.S.G. § 2B.1(b)(10)(C). The USSC stated the amendment was intended to "narrow" the offense characteristic because "prior to the amendment . . . court had applied this

[102] *Id.* at 50.
[103] *Id.* at 37.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

enhancement on the basis of the sophistication of the overall scheme without a determination of whether the defendants' own conduct was 'sophisticated'."[104] Thus, the clarified enhancement "better reflects the defendant's culpability and will appropriately minimize application of this enhancement to less culpable offenders."[105]

Here, there is no evidence that Matthew intentionally engaged in use of a proxy server in order to conceal himself to the objects of the charged conspiracy.

An assessment of Matthew's intent is crucial here, because, as discussed above, he had been using proxy servers long before the charged acts, when one was installed on his computer by an IT Manager at Fox40. Moreover, his initial stated intent was to watch foreign news on his computer, a valid and common purpose for a VPN. There is no showing, not even circumstantially, of his intent. There has been no showing that he created the code for the proxy server, or that he installed it, or that the means of installing it or using it were complex.

3. <u>There was no Showing of Keys' Specific Intent that he Engaged in or Caused the Sophisticated Means</u>

It is for this same reason that Matthew's sentence cannot be enhanced based on his "enlist[ing] the services of highly skilled hackers to carry out his ploy." (PSR at 8). The precise intent element added to the guidelines requires that the defendant himself must have engaged in or caused the sophisticated means. The PSR makes no mention of what sophisticated means the "hackers" used as part of the scheme, nor does it explain how any of that behavior would be attributable to Matthew. Without showing this specific intent, others' use of sophisticated means cannot form the basis of a sophisticated means enhancement for him.

4. <u>Use of Proxy Servers are Common and Ordinary</u>

The use of a proxy server is not categorically a sophisticated means, because it is so common and ordinary that an enhancement on this basis is unjustified.[106] Moreover, VPN proxy servers are typically used in the course of business, for legitimate and legal purposes.

---

[104] United States Sentencing Commission, 2015 amendment to §2B1.1(b)(10)(C), April 30, 2015, pg. 29 available at <http://www.ussc.gov/sites/default/files/pdf/amendment-process/official-text-amendments/20150430_Amendments.pdf>.
[105] *Id.* at 30.
[106] All of Matthew's lawyers uses VPN.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

A "proxy server" is merely a mechanism where one computer communicates with another, the "proxy" and that proxy computer acts on behalf of the original user and sends the results to the user. It has the effect of creating another layer of identification, or protection, for the original user, but does not make detection impossible. Moreover, this layer of identity protection is not the only reason that these services are used. For instance, many companies use VPNs for security and convenience, such as allowing employees remote access to the company's servers when they travel. Of course, these employees are using laptops which may also be used for personal purposes. VPN programs often run transparently, as a background process on the computer. Thus, many users of proxy servers are hardly aware that they are using them. Employees at FOX40, the victim in the charged offenses, used the same kind of proxy devices, which were installed by FOX40's IT Manager for investigative and journalistic uses.

A proxy server requires no technical sophistication on the part of the user, no more than for any of the technologies we all use on a regular basis. We all use sophisticated technology. The computers we use are sophisticated, and so are our smartphones. The cars we used to get here are sophisticated, as are the many computerized features in the car. There are sophisticated security features enabled on each of these devices, to prevent theft, identify fraud, and other abuses of our privacy. We even use sophisticated technology to keep our homes safe, and while this technology is becoming increasingly more advanced, is also becoming more commonplace and easy to use. To argue that each of these uses is a "sophisticated means" would mean that ordinary everyday behavior, otherwise protected and even encouraged, is appropriate to enhance a criminal sentence.

The "sophisticated means" enhancement could not possibly have been intended to encompass such commonplace use of a device that requires no sophistication on the users' part. The amendments to the Sentencing Guidelines reflect that this enhancement was meant to be narrow, so as to exclude from its scope this type simple behavior that is not ordinarily discouraged. Thus, it is an error to enhance Keys's sentence based on his use of a proxy server.

5. <u>Fake Email Addresses</u>

Lastly, the PSR reflects that Keys's use of "fake email addresses" as a factor in determining that he used sophisticated means in connection with the charged offense. If, by "fake email address," the

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

PSR means the use of aliases like "cancerman4099" and "foxmulder4099" in his email addresses, there is nothing "fake" or sophisticated about using a clever alias for an email address. For instance, in the email list of FOX40 viewers introduced as Government Exhibit 108, the email addresses include thevulture209@yahoo.com and jumpy_frogs_17@yahoo.com. This type of alias is common in email addresses, especially on publicly available email services such as Yahoo! mail or Gmail. There has been no evidence to show that there is anything out of the ordinary, let alone sophisticated or "fake", in using these kinds of email addresses. Even council uses fake email addresses to send spam messages to such that they do not clog up his inbox.

B. THERE IS NO BASIS FOR AN ENHANCEMENT FOR AN "AGGRAVATING ROLE," BECAUSE THE ACTIVITY DID NOT INVOLVE FIVE OR MORE PARTICIPANTS AND KEYS DID NOT EXERCISE MANAGERIAL OR SUPERVISORY CONTROL

The PSR recommends a three level enhancement on the basis that Keys "was a manager or supervisor of criminal activity involving five or more participants" under § 3B1.1(b). Its justification is that the "defendant obtained access into a chat room and communicated with at least five members/associates of Anonymous, whom he encouraged to deface the Los Angeles Times website." (PSR at 8). This enhancement is improper because it includes numerous people who bear no criminal responsibility for the charged offenses, played no role in the conspiracy, and were not members of any conspiracy. This inclusion contradicts the Sentencing Guidelines. Moreover, Keys's activity does not rise to the level of management or supervision.

1. **The Charged Activity Did Not Involve Five or More Participants Under the Sentencing Guidelines, Because Mere Presence in a Chatroom Cannot Make Someone Bear Criminal Responsibility**

To qualify as a "participant" for the purposes of this enhancement factor, it is not sufficient to have been in a chatroom where the "criminal activity" was discussed. The Commentary to the Sentencing Guidelines states that a "'participant' is a person who is criminally responsible for the commission of the offense…", adding that "[a] person who is not criminally responsible for the offense…is not a participant." §3B1.1, Commentary, Application Note 1.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Thus, the USSC has emphasized that participants are limited to those who are criminally responsible for the commission of the offense. See, e.g. *United States v. Anderson*, 942 F.2d 606, 616 (9th Cir. 1991) ("Based on this construction of the guideline, we have to conclude that the district court incorrectly applied § 3B1.1(c) so as to adjust Anderson's offense level upward by two points on the assumption that the person with respect to whom he was a leader, organizer, supervisor or manager need not have been criminally responsible for the commission of the offense"); *United States v. Ware*, 577 F.3d 442, 453, 2009 BL 176479, 11 (2d Cir. 2009) ("the record does not indicate that they could be considered "participants" within the above Guidelines definition of that term, for we see no indication in the record that they would be criminally liable"). To be a participant, a party must not only have been aware of the objective, but must have knowingly offered their assistance.[107]

However, the only person who contributed anything to the charged offenses was "sharpie," the chatroom participant who accessed the system to "deface" the LA Times website, and who has otherwise not been identified, and "sabu," who subsequently became a government informant. There were other usernames in the chatroom, but none of them had any active participation in accessing the Fox40's Content Management System. Some of them did no more than make a glib comment, or express words of approval. There is little communication between AESCracked, the username attributed to Matthew Keys, and most of the other persons in the chatroom. None of the usernames in the chatroom have been identified, and there is no way of even knowing if they are separate individuals. It is insufficient that they appear to have cheered on the activity, because in order to be a participant one must have actively participated.

In order to find that "AESCracked" was the manager or supervisor of five or more participants, the PSR must determine that each of these usernames bore criminal responsibility for the charged offenses. This would be online equivalent of finding that each of ten persons in a room was responsible for crimes that only two or three of them discussed and planned, merely because they were in listening distance and they were presumed to be sympathetic to the true participants. *See United States v. Mann*, 161 F.3d 840, 867 (5th Cir. 1998) ("A finding that other persons 'knew what was going on' is not a

[107] *See* United States Sentencing Commission, *Aggravating and Mitigating Role Adjusting Printer*, available at http://www.ussc.gov/sites/default/files/pdf/training/primers/Primer_Role_Adjustment.pdf

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

finding that these persons were criminally responsible for commission of an offense."). But at least in a physical world example, each person can be identified and their actual activities assessed. In a virtual chatroom, the "presence" itself cannot be counted as participation. In fact, it is not even known for sure how many usernames represent unique individuals. The enhancement factor could not possibly have been meant to sweep this broadly.

2. **Keys Did Not Supervise or Manage Participants in Criminal Activity**

Moreover, there is no evidence that Matthew "supervised" or "managed" any individuals. *See, e.g. United States v. Woods*, 335 F.3d 993 (9th Cir. 2003) (finding that enhancer did not apply because defendant did not manage or supervise participants). In order for this enhancement factor to apply, the court must identify a participant over whom defendant exercised managerial or organizational control. *See United States v. Helmy*, 951 F.2d 988, 997 (9th Cir. 1991) ("Consistent with the purposes of Part B, we hold that in order for a defendant to receive an adjustment under § 3B1.1(b) for his role as a manager or supervisor, the defendant must have managed or supervised at least one other participant--that is, a person who was criminally responsible for the commission of the offense"). The adjustment does not apply to a defendant who "merely suggests committing the offense." USSG §3B1.1, Commentary, Application Note 4.

As discussed above, most of the so-called "participants" in the offense were merely usernames in a chatroom that did little more than comment on the ongoing discussion. AESCracked did not have any managerial control over them, and neither did Matthew. He did not know who they were, and did not interact directly with most of them. The only people with whom he discussed the activities were "sharpie" and, to a lesser extent, "sabu" and "kayla." Only one of those individuals, based on the evidence, actually entered into the Content Management System. Matthew did not manage or control "sharpie" when the CMS was entered.

3. **The Activity was Not "Otherwise Extensive"**

Although the PSR does not mention it, the Government may argue that, although there were fewer than five participants, the managerial control was "otherwise extensive" under § 3B1.1(b). However, this subcategory generally requires that there are multiple participants and that there is managerial and supervisorial control. As discussed above, neither of these is true. Most of the Courts of

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Appeals follow the test expressed by the Second Circuit in *United States v. Carrozzella*, 105 F.3d 796 (2d Cir. 1997), which held that "otherwise extensive" requires, at a minimum, "a showing that an activity is the functional equivalent of an activity involving five or more participants." There is no functional equivalent to such an activity, where only one participant in the chatroom actively participated in the activity encouraged by AESCracked, the rest of the persons were merely commenting about it in a chatroom.

Thus, there is no basis for the three-point enhancement under § 3B1.1(b).

C. THE PSR LOSS CALCULATION IS CONTRARY TO SENTENCING LAW AND POLICY AND SHOULD BE REDUCED

The loss enhancements under USSG §2B1.1 were initially designed to address traditional theft, fraud, and embezzlement offenses. These offenses traditionally result not just in a loss for the victim, but also a gain for the perpetrator. While certain offenses under the CFAA may involve an analogous transfer of funds, or an intentional destruction of valuable property, the statute's broad nature covers many offenses which do not. *See* 18 U.S.C. § 1030. Here, the offenses charged are far more similar to vandalism or trespassing than theft or fraud, and are not warranted as a matter of policy. They will also have an extremely disproportionate effect on the sentencing range. With what is essentially "digital vandalism," it is arguable no loss was intended, and certainly a loss in the amount claimed here was neither intended nor reasonably foreseeable. It is also incredibly difficult to establish, and has not been established here, whether the alleged loss included only the reasonable costs to a victim. Applying these enhancement levels for speculative, unintended, and unforeseeable costs and losses creates a perverse sentencing structure that unduly punishes otherwise *de minimis* CFAA offenses.

1. The Loss Calculations Fail to Meet Any Appropriate Burden of Proof

At trial, prosecution witnesses claimed the offenses caused over $900,000 in loss to the victim companies. For sentencing purposes, the 9th Circuit generally accepts a preponderance of the evidence standard as the burden at sentencing, however "a heightened burden may sometimes be required … to satisfy due process concerns." … where a sentencing factor would have an extremely disproportionate effect on the sentence." *United States v. Staten*, 466 F.3d 708, 717 (9th Cir. 2006); *See United States v.*

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Kilby, 443 F.3d 1135, 1140 n. 1 (9th Cir.2006). For factors which have an extremely disproportionate effect on sentencing, the 9th Circuit applies a clear and convincing evidence standard. *United States v. Staten*, 466 F.3d 708, 717 (9th Cir. 2006).[108] Where a sentencing enhancement creates a greater-than-four-level increase and more than doubles the potential sentence, that enhancement likely has a disproportionate effect on sentencing. *See United States v. Staten*, 466 F.3d 708, 717-18 (9th Cir. 2006) (finding disproportionate effect for a greater-than-four level enhancement that more than doubled the sentence); *see also United States v. Dare*, 425 F.3d 634, 642 (9th Cir. 2005) (laying out a 7-factor totality of the circumstances test for disproportionate effect). Here, the clear and convincing evidence standard is appropriate, as the loss enhancement has just such a disproportionate effect. It represents a 10-level increase and nearly triples the recommended sentence, moving the guidelines range from level 19 (30-37 months) to 29 (87-108 months). (*See* PSR, p. 9, ¶ 24.) The evidence offered to support these loss claims fails to meet either standard.

The prosecution's evidence to support their loss claim fails to satisfy either standard. It includes no billing records or other business records beyond an unattributed, undated spreadsheet and a handful of emails. There is no way to tell whether these time entries were directly related to the response, or how much of a given entry was directly related. The jury was never asked to endorse any specific amount beyond the $5,000 minimum for a felony conviction, so the verdict does not endorse any specific number for loss. The claimed losses are simply not established by the evidence, and certainly fail to establish a loss amount by clear and convincing evidence.

2. Unrelated Costs Should be Excluded from the Loss Calculation

Additionally, under USSG §2B1.1, the loss amount must be reasonable, and should exclude, for example, frivolous or unnecessary costs or those not reasonably necessary for incident response or investigation. The Court should look to the fair market value of any "property unlawfully taken … or destroyed" or, for proprietary information, the "cost of developing that information or the reduction in value … that resulted from the offense." *See* U.S.S.G. § 2B 1.1 cmt. n.3 (C)(i), (ii); *United States v.*

[108] Although *United States v. Jenkins* suggests this standard is not applied for conspiracy offenses, that case did not feature a loss calculation which had an extremely disproportionate effect on sentencing, and is thus distinguishable from Mr. Keys's matter. *See* 633 F.3d 788, 808 (9th Cir. 2011)

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Nosal, No. CR-08-0237 EMC, 2014 WL 121519, at *3 (N.D. Cal. Jan. 13, 2014). Additionally, for CFAA related loss, the Court should consider "only those costs that were 'reasonably necessary,' and only those costs that would 'resecure' the computer to avoid 'further damage.'" *United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000). Where the prosecution has not established that certain costs meet one or the other of these criteria, those costs should be excluded from the loss calculation.

The PSR rightly disregards the companies' most nebulous loss claims, such as a decline in morning television news ratings and a vague "database loss in iPad contest." (*See* PSR, p. 7, ¶ 15.) However, it incorrectly includes several loss claims that either fail to meet the appropriate burden of proof or are beyond the scope of loss under USSG §2B1.1.

The PSR incorrectly includes the costs associated with "rebuild[ing] the database." *Id.* Nowhere does it say which database. The undated spreadsheet does not specify this either. In fact, nowhere else in the record seems to clarify what database this cost may refer to. Nowhere does the record establish that any database was "deleted" or needed to be rebuilt. The record contains few mentions of databases at all, and none are alleged as deleted or lost. One database mentioned at trial was the Green Links email address database, and Brendan Mercer admits he was unaware of any deletion of that database or any of its entries. (TR, p. 149; p. 177.) Another witness, Mr. Comings of Tribune Publishing Co., later described the CMS as sharing "a common database." (TR, p. 248). At one point, a witness describes the email list database being "compromised" but in context it is clear they mean the database's information was accessed, not that the database or any information within was deleted. (TR, p. 707). At most, the record supports that the CMS database, "Green Links" email address database, or both may have been accessed, but nowhere does the record suggest any database was deleted.

The Final PSR Response letter itself notes that the "$200,000 figure to 'locate vendor and rebuild new database.'" is uncorroborated by any documents from the victim. These documents have not been provided, nor does the record reflect any database deletion. (*See* U.S. Probation Office Response to Objections, Dec. 30, 2015 (ECF # 127-3), at p. 2.) Where there is no proof of deletion, and no deletion is described in the record, it would be improper to include this figure in Matthew loss or restitution amounts.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

The PSR also mistakenly includes the time-value of "telephone calls, meetings, and emails," which are not contemplated by USSG §2B1.1. These are outside the realm of "reasonable costs to any victim" under the guideline section for 18 USC § 1030 offenses, which includes costs directly related to incident response, but not peripheral or administrative activities. *See* USSG §2B1.1, Application Note 3(A)(v)(III). Including these peripheral activities in the loss calculation would encourage unscrupulous victims to increase their restitution through unrelated or unnecessary meetings and correspondence.

Sentencing policy and the balance of justice weigh against applying these enhancements in a minor CFAA offense such as this. However, if the enhancements for loss are to be strictly applied according to the guidelines, they should be similarly limited by those guidelines and the relevant burden of proof. These loss entries, for an unspecified and unsupported database "deletion" and for administrative tasks at most peripheral to incident response, should not be included in the final loss number. To include them would be unjust, unsupported by the evidence, and against both the spirit and letter of the Sentencing Guidelines.

With these items excluded, assuming the other loss items can be established by clear and convincing evidence, the correct loss amount would be at most $19,591.00, resulting in a 4-point enhancement. *See* USSG §2B1.1(b)(1). This number best reflects a strict adherence to the Sentencing Guidelines, exclusive of unsupported or out-of-scope loss claims.

II. THE STATUTORY SENTENCING FACTORS IN 18 U.S.C. § 3553(a) REQUIRE A SENTENCE BELOW THE GUIDELINES RANGE.

The Sentencing Guidelines are not mandatory. It is always within the discretion of the court to avoid injustice which would result from their rigid application. In fact, it constitutes reversible error for a court to treat the guidelines as mandatory and fail to acknowledge any mitigating factors.

> "[i]t would be procedural error for a district court to fail to calculate — or to calculate incorrectly — the Guidelines range; to treat the Guidelines as

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

> mandatory instead of advisory; to fail to consider the § 3553(a) factors; to choose a sentence based on clearly erroneous facts; or to fail adequately to explain the sentence selected, including any deviation from the Guidelines range. *United States v. Autery*, 555 F.3d 864, 869-870, (9th Cir. 2009)."

Under § 3553, a court considers the following factors:

1. the nature and circumstances of the offense and the history and characteristics of the defendant
2. the need for the sentence imposed to: (A) 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; (D) and 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…the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines;
5. any pertinent policy statement issued by the Sentencing Commission
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.

A. THE NATURE AND CIRCUMSTANCES OF THE OFFENSE AND THE HISTORY AND CHARACTERISTICS OF THE DEFENDANT.

Under 18 U.S.C. § 3553(a)(1), the court is required to consider "the nature and circumstances of the offense and the history and characteristics of the defendant."

1. <u>THE OFFENSE.</u>

As discussed above, the offense at issue here involves the changing of a few words in a Los Angeles Times website article that was easily restored within 40 minutes. The only reason it took 3

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

minutes to restore, and not 15 seconds, is because the editor on duty decided to re-write the headline several times.

2. THE DEFENDANT.

Matthew's background as a journalist is discussed above in the facts section. Matthew is not a "hacker." He is not a member of Anonymous, and never has been. The story told by the Government at trial is one of someone who used his journalistic skills to infiltrate into a closely knit group of newsworthy persons, communicate with a couple of members, and develop a story. The Government's story is of someone who, at beat, unfortunately, got carried away with his work. *See, e.g. United States v. Autery*, 555 F.3d 864, 875 (9th Cir. 2009) (affirming District Court's departure from the sentencing guidelines in child pornography case because defendant "did not fit the profile of a pedophile" and thus did not pose a great threat to society as others who the court had sentenced under the crime). If Matthew is given probation, he will only do what he has been doing for more than a decade, before and after his prosecution – engage in journalism. *See, e.g. United States v. Johnson*, 391 Fed. Appx. 659, 660 (9th 2010) (affirming District Court's departure from the Guidelines where defendant's "post-arrest conduct had been 'very impressive,' 'unique,' and 'extraordinary'" and co-defendants continued to engage in criminal activity).

B. 18 U.S.C. § 3553(a) Factors

Witnesses testified at trial that the change to the Los Angeles Times headline was viewable to the public for a total of approximately 40 minutes. The body of the article was not edited. Additionally, witnesses testified that because of the lapse of security in the Content Management System, they conducted many hours of work in order to fix a system, mostly implementing security measures that should have been in place in the first instance but were not. They also testified that they received the email from a colleague at Fox40 to record all their time so that they can hand to the federal authorities, because they needed to bulk up their "loss" numbers in order to prosecute Matthew. Altogether, the defense agrees with the government that "this not the crime of the century."

Moreover, there is no deterrent purpose in Matthew's imprisonment that is proportionate to the harm caused to Fox40 or that justifies the damage that a lengthy prison sentence will do to Matthew. His journalism career, to which he has dedicated his whole life, has been undermined. He lost his job at

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Reuters. The Department of Justice, along with his former colleagues who testified against him, have branded him as nothing more than a criminal.

In any circumstance similar to Matthew's, a former employee suspected of causing harm to a company, the imposition of draconian prison sentences will not further the purposes of criminal justice. The vast majority of companies under similar circumstances may, at most, seek civil damages against the former employee for their perceived losses. Most people involved in these kinds of disputes do not want their former employees to go to jail, even if they are angered by the employee's actions. The knowledge that a criminal investigation can lead to prison sentences greater than five years will deter many people, including employers, from coming forward to the authorities – that is, all but the ones with the most personal of axes to grind. Thus, the supposed deterrent effect of a lengthy prison sentence results in the unintended consequence of fewer prosecutions for harmful activity.

Matthew has no criminal record, and has never engaged in the activity he was convicted for either before or after the events in question. He wants nothing more than to continue being a journalist. A sentence of probation, with a strict warning from the court on the consequences of any criminal activity, will be sufficient to deter him. *See Autery*, 555 F.3d at 876 ("It is said that there is nothing like being sentenced to hang in the morning to focus a man's thoughts, and it is improbable that the district court's stern warning will be an ineffective deterrent in this case").

Specific deterrence is neither appropriate nor necessary in this case. Nor is general deterrence appropriate in that we have extensively traced the history of Anonymous prosecutions above and shown that the aims of general deterrence have already been served, and they have been served effectively. Those that did not receive prison time have fared as well as those who did. General deterrence has undisputedly not only been served by those punished before him, but those prosecutions have been so widely publicized in news articles, books, and documentaries that if general deterrence was not effective in those prosecutions it will not be effective at all. Matthew's conviction comes out of a time and public perception that caused a group mentality which not only allowed such actions, but even cheered them on. Those days have passed. With the March 6, 2012 revelation that Monsegur was a government informant, the reckless and unabated hacking of the Anonymous "hacktivist" era ended. General deterrence has been served by other, more serious, cases that have come before Matthew's.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

The events at issue here occurred in the winter of 2010. It is now 2016. He is at no risk of reoffending. Matthew was in the Internet Feds chatroom as a journalist. It was important for him to participate in chats as an embedded journalist to gain the trust of the subjects he was writing about. Indeed, his information was used widely and led to a greater understanding of a mysterious and shadowy hacker collective. With the exception of the conviction here, Matthew has no criminal history.

The public needs no protection from Matthew. Rather, he has sought to benefit the public by exposing truth through his journalism. He has shown over the last 5and 1/2 years that the need for rehabilitation is not present in this case.

Borrowing from *United States v. Bergman*, 416 F.Supp. 496, 498-99 (S.D.N.Y. 1976), which some say is the quintessential judicial sentencing memorandum, defendant offers the following:

> "The court agrees that this defendant should not be sent to prison for 'rehabilitation.' Apart from the patent inappositeness of the concept to this individual, this court shares the growing understanding that no one should ever be sent to prison *for rehabilitation*. [*See* 28 U.S.C. § 994(k).] That is to say, nobody who would not otherwise be locked up should suffer that fate on the incongruous premise that it will be good for him or her. Imprisonment is punishment. Facing the simple reality should help us to be civilized. It is less agreeable to confine someone when we deem it an affliction rather than a benefaction. If someone must be imprisoned for other, valid reasons we should seek to make rehabilitative resources available to him or her. But the goal of rehabilitation cannot fairly serve in itself as grounds for the sentence to confinement.
>
> Equally clearly, this defendant should not be confined to incapacitate him. He is not dangerous. It is most improbable that he will commit similar, or any, offenses in the future. There is no need for 'specific deterrence.'"

Matthew understands that if he is to be imprisoned in this case it will be to serve the ends of "general deterrence," which is to say that it will exemplify that this is a wrong that one cannot commit without suffering sanction of a penal nature in addition to the other sanctions that naturally and judicially flow from the sort of act that defendant has been convicted of committing.[109] Even so, it is of great consequence that Matthew is now a felon. None of the top news organizations will now touch

[109] Subections 3553(a)(2)(A) and (B) track this line of thought. Whatever the court decides in terms of punishment, it will not alter the fact that Mr. Keys is a felon, and will suffer the consequences thereof over the rest of his life. This act, committed at 23 years old, will likely ruin his prospects of doing the important work at the pinnacle of his profession that he dreamed of doing.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

him. He had already been employed by Reuters, the largest news organization in the world. Now he is relegated to self-published freelance journalism and companies willing to take risks.

Once again, defendant borrows from *United States v. Bergman*, *supra*, 416 F.Supp. at 498-99, to offer the following:

> In cases like this one, the decision of greatest moment is whether to imprison or not. As reflected in the eloquent submissions for defendant, the prospect of the closing prison doors is the most appalling concern; the feeling is that the length of the sojourn is a lesser question once that threshold is passed. Nevertheless, the setting of a term remains to be accomplished. And in some respects it is a subject even more perplexing, unregulated, and unprincipled.
>
> Days and months and years are countable with a sound of exactitude. But there can be no exactitude in the deliberations from which a number emerges. Without pretending to a nonexistent precision, the court notes at least the major factors.
>
> The criminal behavior, as has been noted, is blatant in character and unmitigated by any suggestion of necessitous circumstance or other pressures difficult to resist. However metaphysicians may conjure with issues about free will, it is a fundamental premise of our efforts to do criminal justice that competent people, possessed of their faculties, make choices and are accountable for them.

Matthew must reluctantly agree with the above statements and acquiesce that it would be unjust to not hold him accountable in any respect. As the Government told the press, he will at least receive probation. Notwithstanding the fact that he may disagree with the jury verdict, he respects the justice system and accepts their judgment. He was found guilty at a jury trial. Accordingly, he stands before the court a guilty man. Even so, the events here do not merit a sentence that includes actual imprisonment. There are situations wherein the age, background, and specific criminality of a defendant would militate towards a simple probationary sentence with conditions. This is just such a case.[110] Matthew was significantly less culpable than any other participant in the criminality of Anonymous during the entire "Hacktivist Era" of the collective, defined as September 21, 2010 to March 6, 2012. Indeed, Matthew does not identify as a member of Anonymous, he identifies as a journalist who studied Anonymous for less than a month in the Internet Feds chatroom. But when compared with each and every other conviction, his actions were *de minimus* compared with any even remotely similar case.

[110] See the Koon brief filed under seal concurrent herewith

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Matthew background, other good acts and prospects call out for him to not be removed from society for any period of time, but rather to be placed on probation; or at most on house arrest for a period of time.

For reasons discussed above, there is no reason to seek out the aims of general deterrence in this case, as this time in hacking and computer misuse history has passed. Even so, it bears mentioning that yielding to a prosecutor's call to "send a message," if any such call is to be made, with this sentence is also improper. *See, e.g.*, *Sinisterra v. United States*, 600 F.3d 900, 910-11 (8th Cir. 2010). A sentencing is an individual determination, based on the facts of the crime and the life and background of the offender. It is contrary to these purposes to ask the court to "make an example" of the defendant for the purposes of deterring other people. Christopher Weatherhead's case in the UK is such an example. His presentence report recommended 3 months[111] after his trial, but the Judge determined he would send a message and sentenced him to 18 months. If a message needed to be sent, it was already received loud and clear in Weatherhead's case.

The need to protect the public from Matthew going forward is nonexistent. Accordingly, a prison sentence would not achieve the aim of protecting the public from Matthew, and may even create a risk where there was none before, prison being the sort of place that turns non-criminals into criminals due to the association of people that don't belong there with those that do. This is admittedly unlikely here, since Matthew has matured and learned from these court proceedings. His interview with the Syrian Electronic Army is a good example of how he has learned to keep an arm's length between himself and his subjects.

Looking at the totality of circumstances present before the court, a probationary sentence is the most appropriate sentence here. Among other reasons, probation will allow the defendant to work and be employed at a productive job, affording the best opportunity for at least some restitution to be swiftly paid. Restitution in this case may be sizeable. Rest assured, restitution will be shouldered by Matthew and it will be a debilitating factor for years, if not a lifetime. The PSR lists his monthly income at approximately $1,700.00 before bills.

[111] Weatherhead was unable to find his copy of the probation report from his case. His memory of the recommendation is crystal clear, 3 months was the recommendation.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

As stated in *Bergman*, the sentence should be calculated "with a sound of exactitude" such that the sentence is no more than is absolutely necessary to send a general deterrent effect to the community, if the court believes one is necessary. Every day counts, as every defendant counts every day they are incarcerated. Looking at all of the relevant factors, zero days in prison should be the sentence affixed in this case. Of course, Matthew could still be subject to house arrest or similar community-based conditions, and would agree that such a punishment would not necessarily be unreasonable in this case.

C. THE KINDS OF SENTENCES AVAILABLE

As the PSR recognizes, the court has many sentencing options. It may within its statutory power impose "(1) straight probation; (2) straight imprisonment; (3) a probationary sentence that includes community confinement or home detention as a condition; or (4) a sentence of imprisonment followed by a term of supervised release that includes community confinement or home detention as a condition." (PSR ¶ 95.) In no event may Defendant's sentence exceed five years. 18 U.S.C. §§ 371.

Admittedly, the Guidelines prohibit a straight probation sentence except where the Guideline range lands in Zone A or Zone B of the sentencing table. U.S.S.G. § 5B1.1(a). Because of the enormous financial loss suffered by Sony Pictures, Defendant's offense level is in Zone D. Thus, the Guidelines do not authorize a probationary sentence. Of course, the Guidelines are advisory, not mandatory. *Booker*, 543 U.S. 220.

Under the statutory provisions—which are mandatory—the court *may* impose straight probation for a Zone D offense. The only offenses categorically ineligible for a probationary sentence are Class A Felonies, Class B Felonies, and offenses which expressly preclude it. 18 U.S.C. § 3561(a). Conspiracy is a Class D Felony and thus is statutorily eligible for probation. *See* 18 U.S.C. § 3559(a)(4). Moreover, in the statutory section defining the duties of the Sentencing Commission, Congress explicitly stated its preference for probationary sentences in cases such as this:

> The Commission shall insure that the guidelines reflect the general appropriateness of imposing a sentence other than imprisonment in cases in which the defendant is a first offender who has not been convicted of a crime of violence or an otherwise serious offense, and the general appropriateness of imposing a term of imprisonment on a person convicted of a crime of violence that results in serious bodily injury. 28 U.S.C. § 994(j).

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

The court has at its disposal a wide range of sentencing options, including straight probation. Despite the Guidelines' advice to the contrary, Congress' explicit preference for probationary sentences for nonviolent, first-time offenders should guide the court in making its choice here.

D. THE NEED TO AVOID UNWANTED SENTENCING DISPARITIES AMONG DEFENDANTS WITH SIMILAR RECORDS WHO HAVE BEEN FOUND GUILTY OF SIMILAR CONDUCT

The Supreme Court has emphasized that "extraordinary circumstances" are not a prerequisite to upholding a sentence outside the Guidelines. *Gall v. United States*, 128 S.Ct. 586, 594 (2007). Indeed, sentences outside the Guidelines are subject to the same abuse of discretion standard as those within the Guidelines. *Id.* at 596 (noting that "abuse-of-discretion standard of review applies to appellate review of all sentencing decisions — whether inside or outside the Guidelines range"). And where the sentence under review is outside the Guidelines, we may not presume the sentence is unreasonable. *Id.* at 597.

Under § 3553(a)(6), the court must also consider sentences given to defendants with similar records who engaged in similar conduct. As discussed above, the sentences meted out to LulzSec, and other Anonymous hackers, for much worse conduct were significantly lighter than what the PSR recommends.

The obvious starting point is to consider the sentences imposed on Internet Feds / LulzSec / Anonymous persons who engaged in similar type conduct – or much worse conduct – but received more reasonable sentences than the one proposed in the PSR – or even the one proposed by the Government.

Defendant deserves a much lighter sentence than the ones imposed on each and every member of Anonymous during the so-called hacktivist period of September 21, 2010 to March 6, 2012.

"[A]s a further deterrent, the district court threatened that if Autery violated any of the conditions of his probation, he would "be back before me and receive the maximum penalty allowed by law. It is said that there is nothing like being sentenced to hang in the morning to focus a man's thoughts, and it is improbable that the district court's stern warning will be an ineffective deterrent in this case." *United States v. Autery*, 555 F.3d 864, 876 (9th Cir. 2009)

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Though Autery was convicted of a computer crime, it a crime that was manifestly different than this one in terms of the conduct, but the offender shares some positive personal characteristics that bear upon this case. As the judge described in that case:

> The court began its analysis of the appropriate sentence by noting that Autery's was "a very difficult case" because there was "no evidence that [Autery] was purchasing evident child pornography involving real children"[Fn. 2: The court may have been referring to the images that Autery received in the government sting operation, images which the government stated were not of real children. Count 3 of the indictment, to which Autery pled guilty, alleges that Autery possessed "visual depictions of actual minors."] (although the court stated that Autery believed they were real children). The court also noted that there was no evidence of Autery's ever abusing family members and that he did not "fit the profile of a pedophile."[112] These facts, the court concluded, made Autery "totally different than what ... [the] court has normally experienced with people who are ordering this sort of child pornography."
>
> The court also described what it considered to be Autery's redeeming personal characteristics: no history of substance abuse, no "interpersonal instability," no "sociopathic or criminalistic attitudes," and that he was motivated and intelligent.[113] The court thought it critical that Autery enjoys the continuing support of his family, especially his wife and children.
>
> The court acknowledged that child pornography is "terrible stuff" and that it believed Autery "ordered it knowing that it was wrong and illegal." But the court found that in

[112] Like the fact that Keys does not fit the profile of either a hacker or a member of Anonymous. He fits the profile of a journalist.

[113] The factors are likewise applicable to Keys.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

several ways, Autery's case differed from the "hundreds and hundreds" of other child pornography cases the court had adjudicated.[114]

The court also believed that Autery could not "be accommodated adequately in a federal institution," and that he needed "outpatient psychiatric monitoring and management" instead. Concluding its sentencing justification, the court stated that it decided on a sentence of probation only "after a lot of soul-searching." It further determined that imposing prison time would create "a much more disruptive situation and, actually, could be more damaging than the rehabilitation [regime the court believed would] work." The court also opined in its written "Statement of Reasons" that the sentence "is fully justified in this exceptional case."

The court observed that the five-year probationary sentence "would be subject to some very special conditions of supervision." It also warned Autery, saying, "believe me, if you have any violation [of those conditions], you'll be back before me and receive the maximum penalty allowed by law."[115] Some of the conditions of probation included a prohibition on viewing any pornography whatsoever and on being within 100 feet of places where minors congregate unless approved by his probation officer. Autery was also not permitted to travel outside the State of Oregon without prior approval. He was required to participate in mental health evaluation and counseling, including psychotherapy, and to take any prescription drugs as directed. He was not permitted to possess any firearm, or to use any computer except for work, or, without approval, any other electronic media — such as a personal digital assistant or cellular phone — with Internet capability. In addition, Autery was not permitted to have "direct or indirect"

[114] It is important to note that Keys' conduct differed in that of any other like person described herein in that it was on a single occasion and not part of a pattern or spree of criminality that others described herein engaged in.
[115] Keys would not object to such a warning.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

contact with anyone under the age of eighteen, except his own children. Finally, Autery was required to register with the state sex offender registry.

555 F.3d 864, 867-868

It is appropriate for a court to take into account other like cases to arrive at a just sentence that is not out of proportion with other apposite cases. In this brief, we have traced what defendants that are similarly situated to Keys have received. The courts have allowed judges to use "their experience of imposing sentences in past, relevant cases as an element in determining the fairness of the sentence for the individual defendant before them. This approach is encouraged by statute, which states that a judge should consider "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct."" 18 U.S.C. § 3553(a)(6). *United States v. Sanchez-Martinez*, 537 Fed. Appx. 693, 695, 2013 BL 211009, 2 (9th Cir. 2013)[116] ("The court simply relied on a formalized version of what all district judges rely upon: their experience of imposing sentences in past, relevant cases.").

Moreover, the facts in *Sanchez-Martinez* were in Matthews' favor. That the Court relied upon a table of cases that both sides were not permitted to see. Here, Matthew has laid out the case that he wishes the court to consider in reaching a just sentence of probation with the possibility of house arrest.

Indeed, while the Court has not sentenced any of the defendants compared to Matthew throughout this brief, the Court is now educated about the "going rate" for these cases around the globe, and has the perspective of what is not just appropriate for the offender, but what is appropriate for the offense when the two are considered together.

The sentencing judge is in the best position to find facts and judge their import under § 3553(a) in the individual case. The judge sees and hears the evidence, and copious evidence has been introduced in this brief of the factors, circumstances and players surrounding the events at issue in this trial. The trial Judge has the superior ability to makes credibility determinations, has full knowledge of the facts and gains insights not conveyed by the record. "The sentencing judge has access to, and greater

[116] See Rule of Appellate Procedure 32.1: (a) Citation Permitted. A court may not prohibit or restrict the citation of federal judicial opinions, orders, judgments, or other written dispositions that have been: (i) designated as "unpublished," "not for publication," "non-precedential," "not precedent," or the like; and (ii) issued on or after January 1, 2007.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

familiarity with, the individual case and the individual defendant before [her] than the Commission or the appeals court." *Rita v. United States*, 551 U.S. 338, 127 S.Ct. 2456, 2469, 168 L.Ed.2d 203 (2007))

Mr. Keys, like almost all of the defendants described herein, has no prior criminal record. This should be considered in Keys case as it was in so many of the other cases involving Anonymous computer activities. It is appropriate to do so not just because it was done for other like defendants, but because a criminal history category of 1 can sometimes account for defendants with some criminal history. IT is not well taken that the criminal history has already been calculated into the guidelines and is therefore not a mitigating circumstance as well. "This argument overlooks the fact that a defendant with a minor criminal history can still fall within Criminal History Level I. *See U.S. Sentencing Guidelines Manual* § 4A1.1 & Ch. 5, Pt. A (2007). Therefore, because Autery's Criminal History Level I did not fully account for his complete lack of criminal history, considering it as a mitigating factor was not redundant or improper. *See United States v. Rowan*, 530 F.3d 379, 381 (5th Cir.2008) (holding probation reasonable for defendant convicted of possessing hundreds of hardcore child pornography images where defendant had no criminal history)."

Keys will not recount the sentences received on three continents by similarly situated defendants who all engaged in significantly more serious and prolific criminality, as it has been so thoroughly briefed and argued *supra* that we do not wish to inundate the court with dualistic facts and arguments. All that remains to be said is that if he receives a guidfeline sentence, or even a 60 month sentence, as the Government has said it will seek, a great and comparative injustice will have been done.

CONCLUSION

For the above reasons, the Court should impose a non-custodial sentence.

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280

Dated March 9, 2016

LAW OFFICES OF JAY LEIDERMAN

By:*/s/Jay Leiderman*
Jason S. Leiderman
Pro Bono Attorney for Defendant
MATTHEW KEYS

TOR EKELAND, PC

By:
Tor Ekeland
Mark Jaffe
Pro Bono Attorneys for Defendant
MATTHEW KEYS

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
Tel: 805-654-0200
Fax: 805-654-0280