UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 16-CR-38 (DEJ)

MARCUS A. OWENS,

Defendant.

MOTION TO DISMISS THE INDICTMENT

For two weeks last year, the United States government operated one of the world's largest child pornography websites. The government placed no limits on the website, allowing more than 100,000 visitors to freely post, view, and share an unknown amount of illegal images and videos. This was distribution of child pornography on a massive scale, likely greater than that of any "distribution" defendant who has ever been prosecuted in this district.

No law permits such behavior. Such actions also contradict the government's long-established position that each and every viewing of child pornography re-victimizes the abused child. These actions were unnecessary to investigate and apprehend many users. And the government knew that it lacked the resources to investigate and prosecute even a simple majority of the site's users.

Federal Defender Services
of Wisconsin, Inc.

In all, the scope and nature of the government's actions were truly unprecedented, with the government committing and enabling crimes on a massive scale. No legal or moral justification excuses the government's behavior. Under Supreme Court precedent, the Court can and should dismiss the indictment in this case.[1]

Factual Overview

The facts of this case are summarized in Mr. Owens's accompanying Motion to Suppress. Regarding the present motion, the relevant facts begin with the FBI taking control of the Playpen website on February 19, 2015. The FBI maintained and operated the site until at least March 4, 2015. Approximately 100,000 users visited during that time (about 50,000 per week), with about "one million total logins." *See* Ex. A, Govt. Response to Order Compelling Discovery, *United States v. Michaud*, Case No. 3:15-cr-5351, Doc. 109 at 4 (W.D. Wa.). Prior to the FBI's operation of the site, the average number of weekly visitors had been just 11,000. *See* Mr. Owens's Motion to Suppress, Ex. B at ¶19.

[1] The defense requests an evidentiary hearing on this motion. Pursuant to Criminal Local Rule 12(c), material disputed issues of fact that the defense requests be addressed at such a hearing include (1) the extent of the pornography distributed from Playpen during the government's operation of the website; (2) how much of the child pornography distributed during that time period was pre-existing images and how much was new material; (3) why the number of users increased so dramatically, and what actions, if any, the government took to affect the number of users; and (4) the overall results of the NIT operation, including how many users were searched and are available for prosecution, so as to determine the overall efficacy of the operation. The defense estimates that such a hearing would require three hours of in court time. After consulting with the assigned government attorney, the defense understands that the government opposes holding an evidentiary hearing on this motion.

By operating the site, the FBI facilitated the uploading and redistribution these images and videos on the Internet. Like any message-board website, the site operator had to approve and provide technical assistance for users to complete these actions. Playpen offered thousands of illicit pictures, videos, and links to additional illegal content (which the government routinely equates as pictures and videos for sentencing purposes), as well as some legal content, such as child erotica, fiction, and technical discussions. The government has estimated that by the time the site closed, it offered roughly 57,000 different pictures, 400 videos, and over a 123,000 links to illicit material. Ex. A at 2-3. In addition, the site allegedly contained "advice" sections about how to avoid detection by law enforcement, and, most disturbingly, how to go about sexually abusing children.

The defense does not know how many different people viewed these pages, or how many images and videos were downloaded. That information has not been disclosed, and the Government has stated that in a companion case that it did not know how many of images, videos, and links had been copied while the site was under its control. *See id.*

The defense offers the following calculation. Given that 100,000 users visited the site during the two weeks the FBI controlled it, and assuming that the site truly was dedicated to child pornography as the government has claimed, one would

assume that most visitors would download many different images or videos during their visits. Assuming a conservative number of only 10 images or videos viewed per visit, this would mean that the government distributed 1,000,000 images of child pornography during this two-week period.

The government also explained that it *could not account* for all of the content that was posted on the site while it was under its control. Much of this content was not tracked by the FBI, and many of the links on the site led to multiple images and videos. Ex. A at 3. What we do know is that under the FBI's watch, the number of weekly visitors to the site increased fivefold, and that the government knowingly distributed an enormous amount of child pornography.

Unlike a typical "reverse sting" operation, the FBI also made no attempt to control or curtail the redistribution of any of the Playpen contraband. This is true despite the fact that the FBI had the power to do so. For example, if could have allowed users to access sub-categories that appeared to contain child pornography while also blocking users from downloading any pictures or videos.

At the end of the two-week period, the FBI shut down the website, even though it had asked for permission to search the site's users for 30 days, apparently recognizing that it could not justify the site's operation.

Investigations into individual users then began, although some investigations may have started during the two-week period. Whether heavy users or individuals who posted new illegal material were targeted first is unknown. The government has stated that it prioritized users who appeared to be actively abusing children. *See* Ex. A at 7-8.[2] But at least some early targets seemed to be passive users—those who spent a few hours on the site and posted nothing. And given the number of users, investigations have necessarily been long in coming. For instance, Mr. Owens's home wasn't physically searched and he wasn't charged until a year after his computer was hacked. Assuming this pace of enforcement is relatively typical, even individuals who have already been charged possessed the child pornography downloaded from Playpen for an extended period of time. This means that these users could have (and many likely did) further disseminate those images.

Moreover, relatively few cases have been brought in comparison to the number of Playpen users. In January of this year, the government claimed that 137 cases had been brought in the United States. Ex. A at 7. This means that of the more than 100,000 users who accessed the website, and presumably downloaded child

[2] As of January, the government claimed that as a result of the operation it "identified or recovered" 26 child victims. *See* Ex. A at 5, 8. Its submission did not differentiate how many victims were "identified" as opposed to "recovered," and did not define these terms. *Id.* at 8.

pornography, the overwhelming majority are still at large, and able to continue spreading the images the government distributed.

Argument

Undoubtedly, the remedy sought in this motion is extraordinary. Yet so was the government's conduct. Investigations typically seek to contain and mitigate the harm caused by illegal activity, not perpetuate that harm exponentially and (according to the Government's own policy) "re-victimize" the children depicted in the images it distributed. Considering the massive amount of illegal pornography distributed by the government, the lack of legal authority to do so, and the government's failure to quickly investigate and stop further distribution of these materials, its conduct merits serious condemnation. Dismissing such a case has been envisioned by the Supreme Court and should be done in this case.

I. The law allows for the dismissal of the indictment in cases where the government acts in an outrageous fashion.

The Supreme Court has long held that the federal judiciary has the power to evaluate a criminal case's entire proceedings to determine whether it "'offend[s] those canons of decency and fairness which express the notions of justice of English-speaking peoples even toward those charged with the most heinous offenses.'" *Rochin v. California*, 342 U.S. 165, 169 (1952) (quoting *Malinski v. People of State of New York*, 324 U.S. 401, 416-17 (1945)). When the government violates

these standards of "decency and fairness" due process concerns are implicated. *See id.* Thus government conduct that "shocks the conscience" may constitute a due process violation, requiring dismissal. *See id.* at 172.

In *United States v. Russell*, 411 U.S. 423, 431-32 (1973), the Supreme Court again reiterated this principle. There it noted that it could envision being "presented with a situation in which the conduct of law enforcement agents is so outrageous" that due process "would absolutely bar the government from invoking judicial processes." *Id.*[3] In short, as Justice Powell put it, police criminal activity needs "reach a demonstrable level of outrageousness before it could bar conviction." *Hampton v. United States*, 425 U.S. 484, 495, n.7 (1976) (Powell, J., concurring); *United States v. Voigt*, 89 F.3d 1050, 1065 (3d Cir. 1996) (dismissal is saved for "only the most intolerable government conduct").

Admittedly, the Seventh Circuit has not yet found a case that satisfies this high threshold. *See United States v. Childs*, 447 F.3d 541, 545 (7th Cir. 2006) (noting that "the Supreme Court has left open" the possibility; discussing the option, but not applying it in a case where the government withheld *Brady* material); *see also United States v. Stallworth*, 656 F.3d 721, 730 (7th Cir. 2011). But the Supreme Court

[3] The Supreme Court has also barred evidence in cases where the government engaged in illegal conduct. *See Nardone v. United States*, 302 U.S. 379 (1937); *Nardone v. United States*, 308 U.S. 338, 341 (1939).

has left the option open: when the government's actions truly shock the conscience, dismissal may be an appropriate sanction. *See, e.g.*, *United States v. Twigg*, 588 F.2d 373, 380 (3d Cir. 1978) (dismissing charges where government helped defendant set up and run a meth lab; government involvement in criminal acts reached "a demonstrable level of outrageousness").

II. The government's actions were unprecedented, illegal, and outrageous.

In this case, the Court should find that the Government's misconduct during the investigation of this case warrants dismissal. While another remedy has been presented to the Court through Mr. Owens's Motion to Suppress, an order of suppression does not adequately address the Government's actions. The Court need only consider some of the Government's own pronouncements about the harm caused by the proliferation of child pornography to realize how troubling the FBI's actions were. One simply cannot reconcile the Playpen operation with the Government's own view of child pornography.

A. The government has long argued that possession or distribution of child pornography is a heinous crime.

For example, the Department of Justice's website explains that child pornography creates multiple layers of abuse. Children "suffer not just from the [original] sexual abuse" but also because they know that "their images can be traded and viewed by others worldwide." Dep't of Justice, *Subject Areas: Child*

Pornography (last visited on July 27, 2016).[4] The circulation and dissemination of such images, according to the DOJ, is a key part of the harm done to the victims. This is because "once an image is on the Internet, it is irretrievable and can continue to circulate forever" and this "permanent record" of abuse permanently alters the child's life. *Id.* Indeed, the DOJ states that victims' "feelings of helplessness, fear, humiliation, and lack of control" stem not just from the original abuse, but from knowing that "their images are available for others to view in perpetuity." *Id.*

The DOJ also routinely emphasizes in its press releases that possessing and circulating pornographic images re-victimizes the children depicted in them. *See* Dep't. of Justice, *Federal and State Authorities Charge 11 Men with Trading Child Pornography* (Apr. 6, 2016) (quoting FBI supervisor stating "[t]he children depicted in these images that were illegally shared are victimized time and time again.");[5] Dep't of Justice, *Ellettsville Man Charged with Production of Child Pornography*, (Apr. 15, 2015) ("Producing and distributing child pornography re-victimizes our children every time it is passed from one person to another").[6] In this district, the U.S. Attorney's Office makes this point at nearly every child pornography

[4] Available at https://www.justice.gov/criminal-ceos/child-pornography.
[5] Available at https://www.justice.gov/usao-cdca/pr/federal-and-state-authorities-charge-11-men-trading-child-pornography-through-use-peer.
[6] Available at https://www.justice.gov/usao-sdin/pr/ellettsville-man-charged-production-child-pornography.

sentencing. *See, e.g.*, *United States v. Soria*, 12-cr-16 (E.D. Wis.), Doc. 54 at 4 ('[A]lthough Mr. Soria's not charged with producing these images, he was a consumer, and every time these images are shared, the impact on victims is compounded. So this is not a victimless crime. It's not a harmless addiction. It's a very, very serious offense."). The argument is frequently used to justify the harsh five-year-mandatory minimum sentences that apply to receipt and distribution charges. *See id.*

This is a perspective that many in the judiciary have come to share. *See* Fed. Bureau of Investigation, *Child Pornography Prosecutions This Week* (May 16, 2014) (district judge telling child pornography possession defendant that "[c]hild pornography is not a victimless crime" and that the defendant "committed one of the most horrendous and atrocious crimes a person could commit against the most vulnerable members of our community"). Thus the Seventh Circuit has explicitly "rejected the notion that merely viewing child pornography is a victimless crime." *United States v. Dean*, 705 F.3d 745, 749 n.3 (7th Cir. 2013); *see also United States v. Norris*, 159 F.3d 926, 930 (5th Cir. 1998) ("The consumer who 'merely' or 'passively' receives or possesses child pornography directly contributes to this continuing victimization."). And the Supreme Court has fully embraced that logic, explaining that circulating child pornography "renew[s] the victim's trauma" and make it

difficult for victims to recover from abuse. *Paroline v. United States*, 134 S. Ct. 1710, 1717 (2014) (victim's suffering was "compounded by the distribution of images of her abuser's horrific acts, which meant the wrongs inflicted upon her were in effect repeated; for she knew her humiliation and hurt were and would be renewed into the future as an ever-increasing number of wrongdoers witnessed the crimes committed against her").

By this logic, or by any logic, distribution is far worse than possession. Given the easily replicated nature of electronic images, just one act of distribution is a "viral" act, allowing an untold number of other people to copy and share that image. Therefore, the distributor of such materials is more culpable, and commits a more serious crime.

Yet even within the category of distribution, there are subcategories. Many "distribution" defendants for example, did not actively barter and trade illegal pornography. Rather, they used Napster-like peer-to-peer programs, where members were free to copy files from each other. *See, e.g.*, *United States v. Gonzalez-Sanchez*, 14-cr-42 (E.D. Wis.), Doc. 19 at ¶6 (describing "distribution" conviction based on government downloading files from the defendant's computer using a peer-to-peer program). Such individuals often don't know if other users copy their files or not. Their culpability is certainly far less than individuals who run entire

websites, thus more actively promoting child pornography. And this more aggravated distribution is exactly what the government did in this case.

The government has often noted that such websites can "encourage" the production and circulation of new pornography. They normalize the behavior, and incentivize individuals to create new material to trade and post. In this case, the FBI has produced no information about how many of the pictures and videos posted on Playpen were "known" images that had been previously circulated on the Internet or if it was aiding and encouraging the production and distribution of new images. The FBI's conduct is all the more troubling in light of the fact that it somehow managed to increase the number of visitors to Playpen from an average of 11,000 per week to roughly 50,000 per week.

The point of highlighting the government's own statements is not to dispute that the possession or distribution of child pornography has harmful effects, or whether the children who are abused in the making of such horrible images deserve the utmost sympathy and care. Instead, the issue is how, while decrying the long-term and widespread consequences of viewing illicit images, the Government can justify its massive distribution of child pornography in this case.

B. The ends of this investigation cannot justify the means.

Clearly, the FBI did this in an effort to apprehend people who view or download child pornography. And it was particularly interested in stopping the ongoing abuse of children. These are undoubtedly laudable goals. But viewed even in a purely utilitarian fashion, those ends did not (and were never going to) justify the means. This is because the FBI simply lacks the capacity to investigate and prosecute the vast majority of Playpen's users in a timely fashion. So the government spread far more child pornography, and enabled far more crimes, than it can prosecute.

To prove this, all one has to do is compare numbers. How many people used Playpen, even before the warrant was issued, and how many cases does the DOJ have the capacity to prosecute? In fiscal year 2014, 75,836 defendants were sentenced in federal court. *See* U.S. Sentencing Comm'n, *Overview of Federal Criminal Cases Fiscal Year 2014*, 1 (Aug. 2015). This provides a rough estimate of that year's successful prosecutions. Only 2.5% of these defendants were sentenced for child pornography offenses. *Id.* at 2. That's 1,896 defendants. So at the time the government requested the warrant, apprehending all of Playpen's roughly 11,000 weekly users would have absorbed the DOJ's entire prosecutorial capacity for child pornography for *more than five years*. But under the government's care, the

number of weekly users exploded to more than 50,000. When it was shut down, the site had more than 200,000 registered users. Prosecuting each of these users would require the DOJ's entire prosecutorial workforce (every U.S. Attorney's Office, every branch of Main Justice, every federal agent) for at least three years.

Imagining that such resources were available, we do not know whether the government even gathered the information needed to launch such investigations. This is because we do not know how many Playpen users the government searched under its legally suspect NIT program. The defense highly doubts that the government had the capacity of searching (let alone further investigating) anywhere close to half of Playpen's ultimate users. This means that, for the sake of a few hundred (or even a few thousand) prosecutions, the government distributed illegal, repulsive, and easily replicated pornography to over 100,000 people, with no consequences.

What's more, as shown in this case, the government had no intention or ability to timely investigate and prosecute the vast majority of these cases. The number of users was simply too large. So cases that were ripe for investigation just sat there. The Court should consider what this means: the government illegally distributed thousands, likely millions, of images of child pornography; and then let the vast majority of those recipients continue to use and view and further share

those images, without limitation and for an extended period of time. Even the small number of users that it chose to prosecute—barring a handful of exceptions—it would get around to them eventually. Meanwhile, those users could continue to view and distribute the free child pornography provided by the government. So the harm caused by the government's actions would continue to spread, perhaps exponentially.

C. Federal law doesn't allow the government to distribute child pornography; rather, the law explicitly forbids it.

The government's behavior also appears to have been flatly illegal. Despite diligent research, the defense has identified no statute that allows the government to distribute child pornography. Multiple statutes govern how law enforcement interacts with such materials. None allow for its distribution, even as part of a misguided "reverse sting." For instance, 18 U.S.C. § 3509(m) expressly requires that "any property that constitutes child pornography . . . shall remain in the care, custody and control of the Government" or a court. This is why defense counsel cannot independently possess such images, even subject to a protective order. (Attorneys have been charged and sued civilly for making fake child pornography as trial exhibits. *See* Pat Murphy, *Court: Lawyer must play $300k for child porn trial exhibits*, Detroit Legal News (Nov. 22, 2012).[7]) And by the letter of the law, the

[7] Available at http://www.legalnews.com/detroit/1369660.

government plainly, repeatedly, and massively violated this statute. Other statutes addressing the government's duties with regard to child pornography include 18 U.S.C. § 1466A(e), 18 U.S.C. § 2252(c), 18 U.S.C. § 2252A(c) and 18 U.S.C. § 2258C(d)-(e). None of these provisions permit the government to freely distribute that material.

And given that Playpen was open to anyone the world over, the government likely violated dozens of international child pornography laws as well. *See, e.g.*, R.S.C. 163.1(3) (Canadian law barring distribution of child pornography); Protection of Children Act, 1978, 1(1)(b) (same, United Kingdom).

D. Alternative methods of investigation existed that would not have distributed child pornography.

In addition, the FBI had other ways of targeting Playpen visitors who wanted to access illegal content. For example, in other investigations, the FBI has monitored child pornography sites and posted links to pictures or videos with explicit titles. When a visitor to the forum clicked on a link, a "Network Investigative Technique" could seize identifying data about the visitor, but the link itself would be blocked or an "error" message would appear. Alternatively, investigators can use a "spoofing" system, where visitors to a target site are secretly redirected to a server with a facsimile of the site, minus any content or links that investigators do not want accessible or downloadable. The government

has also used child erotica or "virtual" child pornography to lure targets in other cases, which would address any concerns agents might have had about "tipping off" suspects if sexual content was removed from the site entirely. *See* Corey Young, *FBI Allowed for More Victimization by Permitting a Child Pornography Website*, The New York Times (Jan. 27, 2016) (discussing some of the investigatory alternatives and criticizing the "immoral and inexcusable" Playpen operation).[8]

What's more, the government maintains that it was authorized to search the personal computers of anyone who merely visited Playpen's home page. If that is true, the government had no need to allow visitors to post new child pornography on the site or download the pornography that was available in specific subdirectories.

E. What occurred here violates DOJ rules and standards regarding "sting" operations, especially those conducted online.

While law enforcement agents often use contraband, like drugs or guns, as part of undercover "buys" or to execute a sting operation, such operations are done with great caution. Usually the government seeks to acquire, not distribute the contraband, thus removing drugs and guns from the street and driving up prices for such items. Agents typically release such items into the community only

[8] Available at: http://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting/fbi-allowed-for-more-victimization-by-permitting-a-child-pornography-website.

when absolutely necessary, and they make every effort to control, track and recover the contraband they use. When such contraband goes missing, it's a scandal. People are fired or transferred, and careers come to a premature end. *See* Dep't of Justice, Office of the Inspector General, *A Review of the ATF's Operation Fast and Furious and Related Matters* (Sept. 2012) (criticizing DOJ's handling of "gun walk" investigations that resulted in the uncontrolled distribution of numerous firearms);[9] John Diedrich & Raquel Rutledge, *Leads on gun stolen from ATF storefront in Milwaukee fizzled out*, Milwaukee Journal Sentinel (Apr. 3, 2013) (automatic weapon stolen from ATF operation).[10]

And this is what happens when the items are not replicable. Guns can be used by only one person at a time. Illegal drugs, while dangerous, can be consumed only once. But electronic images can be copied. One image can be replicated a million times. And unless someone is a prohibited person, merely possessing a firearm is not illegal. Possessing a controlled substance is illegal, but possessing it without using it does little harm. The same cannot be said, by the government's and the federal courts' own logic, with regard to the possession of child pornography.

[9] Available at https://oig.justice.gov/reports/2012/s1209.pdf.
[10] Available at http://archive.jsonline.com/watchdog/watchdogreports/leads-on-gun-stolen-from-atf-fizzled-out-ih9b3i8-201363991.html.

Indeed, the DOJ recognizes that its agents have no ability to control the redistribution of pictures, malware or other contraband once they are introduced to the Internet. As a result, the DOJ itself cautions its attorneys and agents about the harms that can arise from online investigations and requires special approval for any type of "online undercover facility." Dep't of Justice, *Online Investigative Principles for Federal Law Enforcement Agents*.[11] The DOJ's investigative principles emphasize that law enforcement agencies must consider several sensitive issues when determining whether to approve the establishment of an online undercover facility:

> First, online undercover facilities that offer the public access to information or computer programs that may be used for illegal or harmful purposes may have greater capacity than similar physical-world undercover entities to cause unintended harm to unknown third parties. *Because digital information can be easily copied and communicated, it is difficult to control distribution in an online operation and so limit the harm that may arise from the operation.*

Id. at 44 (p. 57 of the PDF) (emphasis added).

The DOJ goes on to caution that using online undercover facilities raises complex legal and policy issues, "especially if law enforcement agents seek to use the system administrator's powers for criminal investigative purposes." These include "unique and sensitive policy issues involving privacy, international

[11] Available at: https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf.

sovereignty, and unintended harm to unknown third parties." *Id.* at x (p. 11 of the PDF). Because of these concerns, the DOJ requires any investigation involving an online undercover facility to undergo a special review and approval process. *Id.* These internal documents have not been produced in any Playpen cases, as far as the defense is aware.

The DOJ's guidelines also compare online "sting" operations with other operations employing criminal tools. Using an example of selling "cloned phones," the DOJ pointed out that agents "can prevent or minimize the potential for harm caused by their activities by, for example, arresting targets before they can use the phones or requesting the cellular carrier to block or limit access by these particular phones to the cellular network." *Id.* at 44 (p. 57 of the PDF). Even when that cannot occur, the harm is constrained by the fact that "a single 'clone phone' can only be used by one individual at a time and cannot be duplicated and redistributed to multiple users." *Id.*

Similar limits, however, are difficult or impossible to impose on online undercover operations, as DOJ cautions in its policy statement:

> [T]he online facility is likely to be automated, making it difficult for the agents to limit who obtains the tools or the damage that the tools end up causing to innocent third parties. Further, unlike the clone phone, the hacker tools can be endlessly replicated and distributed to others in a manner that law enforcement agents cannot easily control.

Id. at 45 (p. 58 of PDF) (emphasis added).

Unfortunately, in this case, the FBI took no measures whatsoever to control the replication and distribution of pictures and videos from its undercover website. And such materials, as the DOJ itself has acknowledged, are viral. They are easily copied, highly sought after, and can encourage further abuse of children. In disseminating this contagious material, the government acted a like modern-day version of the AIDS "Patient Zero" who spread the disease to hundreds of partners. Assuming the stories are true, he was a hedonist, who sought his own pleasure and didn't want to think of the consequences. The government's motivations were certainly higher-minded, but the consequences were similarly disastrous.

F. The government has refused to meet its legal obligation to make restitution.

Finally and somewhat unbelievably, the Government has also so far denied that it has any responsibility to the victims depicted in the pictures that it distributed. Its own mission statements explain that it harmed the lives and mental health of thousands of victims by distributing child pornography. So like any entity that distributes or possesses child pornography, it has a statutory obligation under 18 U.S.C. § 2255 to make restitution to its known victims. Yet despite the DOJ's rhetoric and policy statements discussed above, and despite its position that

it seeks to protect child victims, the government has done nothing to make restitution.

Conclusion

Given the lack of hard data at this point, the ultimate number of images disseminated by the government is unknown. But it can be reasonably estimated that more than 10,000 easily replicable, undying images of child abuse were downloaded over a million times. How many times these images have subsequently been viewed and copied is unknown. And this was allowed, encouraged even, knowing that it couldn't be justified. The government knew that it lacked the resources to prosecute even a fraction of the site's users. It didn't prosecute most cases with any special urgency, thus allowing the images it disseminated to continue to spread unchecked. And the government's conduct appears to have been flatly illegal.

Given the government's consistent position on the "very serious" harm of even viewing (let alone distributing) child pornography, this was unjustifiable hypocrisy. Thousands of children were re-victimized, again and again, and will continue to be, perhaps forever. And the uncontrollable spread of these images will continue to create new criminals. The ultimate harm caused by the government in this case is unknowable, but reasonably appears to be immense.

Defense counsel is not aware of any similar operation occurring in American history. Perhaps the closest comparison is the government's notorious "Fast and Furious" operation.

For these reasons, the Court should schedule an evidentiary hearing to determine the true extent of the harm caused by the Government's investigatory tactics. The Court should then dismiss the indictment if the Court finds that the governmental conduct leading to the charges against Mr. Owens cannot be reconciled with fundamental expectations of decency and fairness.

Dated at Milwaukee, Wisconsin this 1st day of August, 2016.

Respectfully submitted,

/s/ Anderson M. Gansner
Anderson M. Gansner, Bar No. 1082334
FEDERAL DEFENDER SERVICES
OF WISCONSIN, INC.
517 E. Wisconsin Avenue, Room 182
Milwaukee, Wisconsin 53202
Telephone: 414-221-9900
Fax: 414-221-9901
E-mail: anderson_gansner@fd.org

Counsel for Defendant, Marcus A. Owens

Judge Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-5351RJB UNITED STATES' RESPONSE TO ORDER COMPELLING DISCOVERY

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Matthew P. Hampton, Assistant United States Attorney for said District, and Keith A. Becker, Trial Attorney, hereby files this response to the Court's December 15, 2015, order compelling discovery (Dkt. 81):

A. Number of pictures, videos, and links

The Court first ordered the government to provide the defense with the number of child pornography pictures, videos, and links to pictures and videos that were posted on Website A between February 20 and March 4, 2015, "[p]rovided however, if the plaintiff cannot produce the exact picture, video and link totals listed above with reasonable effort, the plaintiff should provide a good faith estimate of the totals." Dkt. 81, pp. 1-3.

Website A was an online bulletin board through which users provided the content of the site by posting messages and/or replies to messages within categories set up by the site

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

administration. In accordance with the site rules and guidelines, users generally posted textual messages in which "preview" images (generally consisting of still frames taken from a video or a selection of images) were embedded, and that included a link to a URL, the address of a website or server at which the videos or images could be downloaded, along with any password necessary to download and decrypt the videos or images.

During the course of the investigation of Website A, before and after its seizure, the FBI expended significant efforts to document and capture as many of the images/videos posted in this fashion by site users as practicable. Given the significant number of users and activity on the website, it was not possible to capture all of that content. To access the images and videos, the agents had to access the website or link contained in the message, download the files or a file "archive" – that is, a compressed file containing numerous other files – and then enter a password in order to access the files. This process could not be automated, meaning that it was necessary for an agent physically to take these steps rather than simply direct a computer to do the work. Moreover, images and videos that were made available by Website A users were generally only available for a limited time. Thus, if the agents were not able to complete accessing all of the website's advertised materials at or near the time of posting, those materials might no longer be available. With that understanding, we provide the following good faith estimates based upon FBI agents' downloads of files made available by the users of Website A through their posts and through the seizure of data from the Website A image and file hosts.

Through the efforts described above, the FBI recovered approximately 48,000 images and 200 videos that were made available by the site's at least 184,000 users between the inception of Website A in August 2014 and its seizure on February 20, 2015. In addition, the FBI was able to recover approximately 9,000 images and 200 videos that were made available by Website A users while it operated under FBI administrative control between February 20 and March 4, 2015. The vast majority of those images/videos appeared to depict child pornography or child erotica. In some instances, particularly with respect to sets of images pertaining to a particular child, children were depicted in various states of undress progressing to nudity and/or sexually explicit activity. This is common among child pornography images.

Website A users posted approximately 110,000 links on the website between August 2014 and February 20, 2015. During the period from February 20 through March 4, 2015,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Website A users posted approximately 13,000 links on the website. As noted above, links posted by Website A users typically pointed either to encrypted archives containing multiple image or video files of child pornography, or to particular image files depicting child pornography. Although FBI cannot specify exactly how many images and videos were contained within each of those encrypted archives, as noted above, FBI was able to recover approximately 9,000 images and 200 videos that were made available by Website A users while it operated under FBI administrative control between February 20 and March 4, 2015.

B. Views and downloads from February 20 through March 4, 2015

The Court next ordered the government to provide the defense with the number of child pornography pictures and videos that were viewed and downloaded from Website A between February 20 and March 4, 2015, or a good faith estimate of these totals. Because of the manner in which Website A works, it is not possible to give an exact total of child pornography images or videos viewed or downloaded by site users during that time period. As noted above, Website A was a bulletin board on which users posted messages with embedded links and preview images. Another user may choose simply to view the preview image that is embedded on a web page without clicking that image or taking an action that would be recorded by Website A. Moreover, there are numerous ways for a user to save or download images contained on a website such as Website A that would not be recorded by the website. For example, a user might "right click" and save an image to the user's computer. The user could also take a "screen shot" of the computer screen, or go directly to the external website where linked images or videos were contained by typing the URL for the site after leaving Website A, and then entering the appropriate password, and downloading the images/videos. With that understanding, we provide the following good faith estimates.

Information about the number of links Website A users clicked on between August 2014 and February 20, 2015, before the FBI was in administrative control of the website, is not available. Between February 20 and March 4, 2015, Website A users clicked on approximately 67,000 unique links on the website. As explained above, links on Website A typically pointed either to encrypted archives containing multiple image or video files of child pornography, or to particular image files depicting child pornography. Of those 67,000 links, 25,000 were links to

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

image files, the majority of which appeared to depict child pornography. The remaining links were to websites, which typically contained the sort of encrypted archives described above.

C. Statistics concerning Website A usage between February 20 and March 4, 2015

The Court next ordered the government to provide the defense with the number of visitors to the site between February 20 and March 4, 2015, the number of total visits, and some measure of the length of visits. Between February 20 and March 4, 2015, approximately 100,000 unique user accounts logged in to Website A, and there were approximately one million total logins. An individual could have more than one user account on the site, so it is not clear how many individuals this actually represents. Website A tracked total time spent on the site by each user during the course of the user's membership. From the inception of the website in August of 2014 until March 4, 2015, site data indicate that its more than 200,000 users aggregately spent approximately seven million hours logged into the site. Based on available data and with reasonable effort, the government cannot provide an estimate of the total or average length of site visits between February 20 and March 4, 2015. Providing such figures would require a manual review of every single session by every single site user in order to total the amount of time spent during each session, and then average that amount of time. That manual analysis has been done for Mr. Michaud (via data that have been provided to the defense in discovery pertaining to his use of Website A) and shows that during his fourteen total sessions on Website A between February 21, 2015, and March 2, 2015, Michaud spent approximately sixteen-and-a-half hours on Website A for an average of 1.18 hours per visit. As previously disclosed, Michaud spent a total of approximately ninety-nine hours logged into the site between October 31, 2014, and March 2, 2015.

D. Mitigation efforts

The Court next ordered the government to provide the defense with a summary of any measures that were taken by the FBI or other law enforcement entities to block access to the pictures, videos and links available on or through the Website A between February 20 and March 4, 2015.

During the brief period when the FBI assumed administrative control of Website A, the FBI did not post any images, videos, or links to images or videos of child pornography. Images,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

videos and links posted by site users both before the FBI assumed administrative control and afterwards, generally remained available to site users.

While Website A operated under FBI administrative control, FBI Special Agents monitored all site postings, chat messages, and private messages twenty-four hours per day in order to comply with Title III monitoring requirements and in order to assess and mitigate any risk of imminent harm to children. In the event that FBI Special Agents perceived a risk of imminent harm to a child, agents took actions to mitigate that risk and immediately forwarded available identifying information, including NIT results, to the appropriate FBI office. Specific actions taken in any particular instance were tailored to the specific threat of harm. The particular actions taken by law enforcement agents in response to particular circumstances are protected by a qualified law enforcement privilege, which the United States hereby asserts. In particular, disclosure of this information at this point in time would alert subjects of ongoing investigations to the particular investigative techniques used by law enforcement in response to such circumstances, creating a risk that criminal suspects will recognize and circumvent such techniques in the future and leading to increased danger of harm to the public, including children. The risk of circumvention of an investigative technique if information is released has been recognized as a factor in applying law enforcement privilege to electronic surveillance. *See United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1986). In any event, no such actions pertained to any postings or messages involving the defendant's known username, Pewter.

E. Reason for shutting down Website A

The Court also required the government to produce the reasons the site was shut down on March 4 (rather than earlier or later). As the government explained to the two separate judges who authorized the NIT and the Title III authorization to monitor site users' communications, the fourteen-day period during which the FBI allowed the operation of Website A to continue was necessary in order to deploy the court-authorized NIT to identify users of this site who, like Mr. Michaud, used Tor to conceal their identity, location, and illegal conduct. Without using the NIT, the identities of the users of Website A would remain unknown because, unlike a non-Tor website, any IP address logs of user activity on Website A would disclose only Tor "exit nodes," which could not be used to locate and identify the actual administrators or users of the site. Further, because of the unique nature of the Tor network and the method by which the network

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

routes communications through multiple other computers, investigative procedures that are usually employed in criminal investigations of this type were tried and failed or reasonably appeared to be unlikely to succeed.

The government demonstrated the necessity of the investigative strategy and technique used in this investigation in the affidavit submitted in conjunction with its Title III authorization. As the government indicated in that affidavit, agents considered seizing Website A and removing it from existence immediately and permanently. In the judgment of law enforcement agents, while doing so would have ended the trafficking of child pornography taking place via Website A, it would have also prevented law enforcement from attempting to locate and identify its users, who were the ones who possessed, and were distributing and receiving, those illicit materials. It also would have frustrated agents' attempts to obtain information that could help identify and rescue child victims from ongoing abuse. Accordingly, it was the judgment of law enforcement that the seizure and continued operation of Website A, for a limited period of time, paired with the court-authorized deployment of a NIT and monitoring of user communications, was necessary and appropriate in order to identify Website A users. The judges who signed the NIT warrant and Title III authorization obviously agreed.

To be sure, shutting down a facility such as Website A would have prevented its unidentified users from continuing to post and disseminate child pornography through that website, but it would not prevent those users from continuing to unlawfully possess and disseminate child pornography by other means. Website A users engaged in that sort of activity before the FBI seized and shut down Website A, and those users who were not identified and apprehended undoubtedly continued to engage in that activity after Website A was shut down, often through other online facilities. For instance, before the February 20, 2015, seizure of Website A, it contained at least 184,000 active user accounts, 103,000 posts, and facilitated access to thousands of images and videos of child pornography. There are currently child pornography bulletin boards operating on the Tor network that are similar in structure and function to Website A, that contain hundreds of thousands of user accounts, tens of thousands of postings, and which facilitate access to thousands of images and videos of child pornography. Law enforcement agents can view and document those websites, their contents, and the child pornography images and videos trafficked through them – but because they operate as Tor

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

hidden services, the location of the computer servers hosting the websites, and the location and identity of their users who are perpetrating crimes against children, and their child victims, are currently unknown.

Stopping the unlawful possession and dissemination of child pornography materials by particular individuals, and rescuing children from the ongoing abuse and exploitation of individual perpetrators, therefore requires more than just shutting down one facility through which such materials are disseminated. Law enforcement must identify and apprehend the perpetrators. Here, the FBI briefly assumed administrative control over an existing facility through which users were already posting and accessing child pornography, for a limited period of time, in order to deploy a court-authorized investigative technique and engage in court-authorized monitoring of user communications, which were necessitated by the particular anonymizing technology deployed by the users of the site, in an effort to identify those perpetrators. This difficult decision, which was disclosed both to the magistrate who approved the NIT and the district judge who approved the Title III monitoring, was amply justified by the particular facts of the investigation.

During the government's operation of Website A, regular meetings were held to discuss the status of the investigation and identification of site users and assess whether the site should continue to operate, based upon a balancing of various factors, to include site users' continued access to child pornography, the risk of imminent harm to a child, the need to identify and apprehend perpetrators of those harms to children, and other factors such as those described above. On March 4, 2015, it was determined that the balance of those factors weighed in favor of shutting down the website.

F. Statistics concerning charges

Although it is not reflected in the Court's written order, during the December 11, 2015, hearing the court also stated: "[i]f specifics are not available, I think also the number of charges arising from this investigation should be – the numbers, only numbers, I am saying – should be provided to the defense." Dec. 11, 2015, Tr. at 34. The investigation into users of Website A remains ongoing. To date, at least 137 individuals in the United States are known to have been charged in connection with the underlying investigation of Website A. That includes thirty-five individuals who have been determined to be "hands on" child sexual offenders, and seventeen

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

individuals who have been determined to be producers of child pornography. More importantly, twenty-six child victims have been identified or recovered from abuse. Individual charging decisions are made at the discretion of United States Attorneys' Offices and/or appropriate state authorities and this does not represent a complete reporting of all individuals who could be charged in connection with the investigation.

G. Documents regarding FBI administrative control of Website A

Although the Court also ordered the government to provide: "All documents relating to review and authorization of the FBI's administrative control of the site by the Department of Justice or other governmental agencies that were involved in the 'Website A' investigation and deployment of the NIT at issue in our case," the Court qualified its directive, stating: "Provided further, that the government need not provide to defense counsel any documents under the above requirement that constitute reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting this case[.] FRCP 16(a)(2)." Dkt. 81 at pp. 2-3.

Discovery materials already provided, including the NIT search warrant and the Title III application paperwork, clearly indicate the scope and purpose of the operation to identify users who were abusing and exploiting children online while masking their location via the Tor network. The NIT search warrant affidavit, which clearly described the operation of the website at a government facility for a limited time in order to identify users, was sworn to by an FBI Special Agent and presented by an Assistant U.S. Attorney from the Eastern District of Virginia and a Trial Attorney with the Department of Justice's Child Exploitation and Obscenity Section. The Title III application and affidavit, which also clearly described the scope and purpose of the operation, including the website's operation at a government facility for a limited period of time in order to deploy a court-authorized NIT to identify users, was submitted by two Department of Justice attorneys, based on an affidavit sworn to by an FBI Special Agent, and approved, as all Title III applications are required to be, by a Deputy Assistant Attorney General of the Department of Justice's Criminal Division.

Although the United States is in possession of documents that would be responsive to the first portion of the Court's order, the United States is not producing those documents at this time pursuant to the second portion of the Court's order, Federal Rule of Criminal Procedure 16(a)(2),

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

attorney-client, work product and deliberative process privileges. *See United States v. Fernandez*, 231 F.3d 1240, 1246-47 (9th Cir. 2000).

DATED this 8th day of January, 2015.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
Matthew P. Hampton
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
Telephone: (253) 428-3800
Fax: (253) 428-3826
E-mail: matthew.hampton@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on January 8, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney of record for the defendant.

/s/ Matthew P. Hampton
MATTHEW P. HAMPTON
Assistant United States Attorney

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800