April 28, 2016

Honorable Paul D. Ryan
Speaker of the House of Representatives
Washington, D.C. 20515

Dear Mr. Speaker:

I have the honor to submit to the Congress the amendments to the Federal Rules of Criminal Procedure that have been adopted by the Supreme Court of the United States pursuant to Section 2075 of Title 28, United States Code.

Accompanying these rules are the following materials submitted to the Court for its consideration pursuant to Section 331 of Title 28, United States Code: a transmittal letter to the Court dated October 9, 2015; a redline version of the rules with Committee Notes; an excerpt from the September 2015 Report of the Committee on Rules of Practice and Procedure to the Judicial Conference of the United States; and an excerpt from the May 6, 2015 Report of the Advisory Committee on Criminal Rules.

Sincerely,

/s/ John G. Roberts

April 28, 2016

Honorable Joseph R. Biden, Jr.
President, United States Senate
Washington, D.C. 20510

Dear Mr. President:

I have the honor to submit to the Congress the amendments to the Federal Rules of Criminal Procedure that have been adopted by the Supreme Court of the United States pursuant to Section 2075 of Title 28, United States Code.

Accompanying these rules are the following materials submitted to the Court for its consideration pursuant to Section 331 of Title 28, United States Code: a transmittal letter to the Court dated October 9, 2015; a redline version of the rules with Committee Notes; an excerpt from the September 2015 Report of the Committee on Rules of Practice and Procedure to the Judicial Conference of the United States; and an excerpt from the May 6, 2015 Report of the Advisory Committee on Criminal Rules.

Sincerely,

/s/ John G. Roberts

April 28, 2016

SUPREME COURT OF THE UNITED STATES

ORDERED:

1. That the Federal Rules of Criminal Procedure be, and they hereby are, amended by including therein amendments to Criminal Rules 4, 41, and 45.

[*See infra* pp. __ __ __.]

2. That the foregoing amendments to the Federal Rules of Criminal Procedure shall take effect on December 1, 2016, and shall govern in all proceedings in criminal cases thereafter commenced and, insofar as just and practicable, all proceedings then pending.

3. That THE CHIEF JUSTICE be, and hereby is, authorized to transmit to the Congress the foregoing amendments to the Federal Rules of Criminal Procedure in accordance with the provisions of Section 2075 of Title 28, United States Code.

PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CRIMINAL PROCEDURE

Rule 4. Arrest Warrant or Summons on a Complaint

(a) Issuance. If the complaint or one or more affidavits filed with the complaint establish probable cause to believe that an offense has been committed and that the defendant committed it, the judge must issue an arrest warrant to an officer authorized to execute it. At the request of an attorney for the government, the judge must issue a summons, instead of a warrant, to a person authorized to serve it. A judge may issue more than one warrant or summons on the same complaint. If an individual defendant fails to appear in response to a summons, a judge may, and upon request of an attorney for the government must, issue a warrant. If an organizational defendant fails to appear in response to a summons, a judge may take any action authorized by United States law.

* * * * *

(c) Execution or Service, and Return.

(1) ***By Whom.*** Only a marshal or other authorized officer may execute a warrant. Any person authorized to serve a summons in a federal civil action may serve a summons.

(2) ***Location.*** A warrant may be executed, or a summons served, within the jurisdiction of the United States or anywhere else a federal statute authorizes an arrest. A summons to an organization under Rule 4(c)(3)(D) may also be served at a place not within a judicial district of the United States.

(3) ***Manner.***

(A) A warrant is executed by arresting the defendant. Upon arrest, an officer possessing the original or a duplicate

original warrant must show it to the defendant. If the officer does not possess the warrant, the officer must inform the defendant of the warrant's existence and of the offense charged and, at the defendant's request, must show the original or a duplicate original warrant to the defendant as soon as possible.

(B) A summons is served on an individual defendant:

(i) by delivering a copy to the defendant personally; or

(ii) by leaving a copy at the defendant's residence or usual place of abode with a person of suitable age and discretion residing at that location and by

mailing a copy to the defendant's last known address.

(C) A summons is served on an organization in a judicial district of the United States by delivering a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process. If the agent is one authorized by statute and the statute so requires, a copy must also be mailed to the organization.

(D) A summons is served on an organization not within a judicial district of the United States:

(i) by delivering a copy, in a manner authorized by the foreign jurisdiction's law, to an officer, to a

managing or general agent, or to an agent appointed or legally authorized to receive service of process; or

(ii) by any other means that gives notice, including one that is:

(a) stipulated by the parties;

(b) undertaken by a foreign authority in response to a letter rogatory, a letter of request, or a request submitted under an applicable international agreement; or

(c) permitted by an applicable international agreement.

* * * * *

Rule 41. Search and Seizure

* * * * *

(b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

* * * * *

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

* * * * *

(f) Executing and Returning the Warrant.

(1) ***Warrant to Search for and Seize a Person or Property.***

* * * * *

(C) *Receipt.* The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property. For a warrant to

use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.

* * * * *

Rule 45. Computing and Extending Time

* * * * *

(c) Additional Time After Certain Kinds of Service. Whenever a party must or may act within a specified time after being served and service is made under Federal Rule of Civil Procedure 5(b)(2)(C) (mailing), (D) (leaving with the clerk), or (F) (other means consented to), 3 days are added after the period would otherwise expire under subdivision (a).

Judge Marsha J. Pechman

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

UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	NO. CR15-00274MJP UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO DISMISS INDICTMENT

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Matthew P. Hampton and André M. Peñalver, Assistant United States Attorneys for said District, and Keith A. Becker, Trial Attorney, hereby files this response to the defendant's motion to dismiss the Indictment.

I. BACKGROUND

The United States charged Bruce Lorente with receipt and possession of child pornography following a search warrant executed at his home during which the FBI seized several digital devices containing illegal child pornography. Lorente also agreed to an interview during which, among other things, he admitted that he had been using the Internet, including the Tor network, to view and download child pornography for years.

The charges arise from an FBI investigation into a child pornography website, "Playpen," operating on the anonymous Tor network. In late February 2015, the FBI

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

seized and assumed administrative control of the site—which had already been operating for six months—for approximately two weeks in order to deploy a court-authorized Network Investigative Technique (the "NIT") and to conduct court-authorized monitoring of user communications to identify Playpen's users.[1]

Importantly, the FBI did not create Playpen, and Lorente had registered as a user long before law enforcement seized it. Indeed, he has admitted to viewing child pornography regularly since 2000. The FBI provided no inducement to Lorente to access child pornography, nor did the FBI post any child pornography or any links to child pornography on the website. Finally, the brief continued operation of the site was necessary in order for the FBI to obtain identifying information about its users, pursuant to court authorization, in light of the nature of the crime and the suspects' use of the anonymous Tor network.

Lorente seeks dismissal of the Indictment for "outrageous government conduct." But as another judge in this district concluded in denying an identical motion in a case arising from the same operation, the government acted reasonably to solve a difficult problem it faced in investigating crimes involving the sexual exploitation of children. Settled Ninth Circuit precedent establishes that a defendant alleging outrageous government conduct must demonstrate that the government has done something that shocks the Court's conscience. This Lorente cannot do, and his motion should be denied.

II. LEGAL STANDARDS

Outrageous government conduct is law enforcement conduct that is "'so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction.'" *United States v. Black*, 733 F.3d 294, 302 (9th Cir. 2013) (quoting *United States v. Russell*, 411 U.S. 423, 431-32 (1973)). Defendants raising such claims must meet an "extremely high standard." *United States v. Garza–Juarez*, 992 F.2d 896, 904 (9th Cir. 1993). Dismissal is "limited to extreme

[1] A more detailed description of Playpen and the investigation of it are contained in the government's response to Lorente's motion to suppress.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

cases" in which the defendant can demonstrate that the government's conduct "violates fundamental fairness" and is "so grossly shocking and so outrageous as to violate the universal sense of justice." *United States v. Stinson*, 647 F.3d 1196, 1209 (9th Cir. 2011) (quoting *United States v. Smith*, 924 F.2d 889, 897 (9th Cir. 1991) (internal quotation marks omitted)).

Significantly, the government has found only two reported decisions in which federal appellate courts have reversed a conviction for outrageous government conduct. *See United States v. Twigg*, 588 F.2d 373, 381 (3d Cir. 1978) (holding government conduct outrageous because it "generated new crimes by the defendant merely for the sake of pressing criminal charges against him when . . . he was lawfully and peacefully minding his own affairs"); *United States v. Greene*, 454 F.2d 783 (9th Cir. 1971) (holding government conduct outrageous where it had initiated a criminal scheme and was involved for two and a half to three and a half years "directly and continuously . . . in the creation and maintenance of criminal operations").

In contrast, there are numerous reported decisions where courts have declined to dismiss an indictment in the face of alleged outrageous conduct—even in cases involving so-called "reverse stings"—where the government initiates the criminal conduct by inventing a fictitious criminal scenario and then prosecutes a defendant who attempts to participate in it. *See, e.g.*, *United States v. Pedrin*, 797 F.3d 792, 794 (9th Cir. 2015) (affirming finding of no outrageous government conduct where an "undercover agent pose[d] as a disgruntled drug courier with knowledge about a stash house . . . containing a large amount of cocaine," suggested "to targets of the reverse sting that they join forces, rob the house, and split the proceeds," and then "arrested and charged [them] with conspiracy" once the targets took "steps to rob the fictional house"); *Black*, 733 F.3d at 302 (affirming finding of no outrageous government conduct in similar fictional stash-house sting operation planned by government agent because, when "presented with the fictitious stash house robbery proposal [the targets] . . . readily and actively" participated in the criminal activity "as willing participants"). The standard is all the higher where, as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

here, law enforcement was not responsible for creating the criminal scheme under investigation. *See, e.g.*, *United States v. Gurolla*, 333 F.3d 944, 950 (9th Cir. 2003) (holding government conduct not outrageous when, as here, "the government merely infiltrates an existing organization, approaches persons it believes to be already engaged in or planning to participate in the conspiracy, or provides valuable and necessary items to the venture").

The Ninth Circuit has identified six factors that guide the outrageousness inquiry:[2]

> (1) known criminal characteristics of the defendant[]; (2) individualized suspicion of the defendant[]; (3) the government's role in creating the crime of conviction; (4) the government's encouragement of the defendant[] to commit the offense conduct; (5) the nature of the government's participation in the offense conduct; and (6) the nature of the crime being pursued and necessity for the actions taken in light of the nature of the criminal enterprise at issue.

Black, 733 F.3d at 303. This is not a formalistic checklist, and assessing the government's conduct is not a bright line inquiry. Rather, it involves an evaluation of the totality of the circumstances based on the facts of each particular case. *Id.* at 302, 304.

Applying these principles, it is clear that nothing about what the government did was unreasonable—let alone outrageous—in light of the problem it faced. In denying an identical motion in *United States v. Michaud*, CR15-5351RJB, Judge Bryan provided as clear an articulation of this as any:

> It is easy to argue, and, my gosh, we hear it in all kinds of cases, that the other side's position is outrageous. Well, you know, that's a high standard. From the standpoint of one who stands between the defendant and the government, and represents neither side, you look at what happened and look inward. I am not shocked by this. I did not find it outrageous.

Ex. 1, Jan. 22, 2016, Hr'g. Tr., p. 43.

---

[2] Perhaps tellingly, Lorente's motion to dismiss neither cites these factors nor makes any effort to illustrate how they would support dismissal of the Indictment in this case.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

III. ARGUMENT

A. The government had ample reason to believe that Playpen users, including Lorente, were unlawfully viewing and sharing child pornography.

The first two factors are "[c]losely related," and they examine whether, at the time the operation commenced, the government had reason to suspect "an individual or identifiable group," and whether that individual or group had a "propensity the government knew about when it initiated its sting operation." *Black*, 733 F.3d at 304. When the government seized Playpen, it admittedly had no reason to suspect Lorente as it had not identified him. It did, however, have ample reason to suspect any member of Playpen (which turned out to include Lorente) was actively viewing and sharing child pornography.

As the affidavit in support of the NIT warrant explained, between September 2014 and February 2015, undercover FBI agents connected to Playpen in order to document its content and attempt to identify site users. Dkt. 48, Ex. 1, p. 13, ¶ 11. Playpen became a focus of investigation precisely because its members were actively advertising, distributing, and accessing child pornography. *Id.*, p. 10, ¶ 6. Images and videos that were advertised, distributed, and accessed through the site were highly categorized according to the gender and age of the victims portrayed—*e.g.*, "jailbait," "pre-teen" and "toddlers"—as well as the type of sexual activity depicted, such as hardcore ("HC") or softcore ("SC") child pornography. *Id.*, pp. 15-17, ¶¶ 14-18. The images and videos comprised all manner of child sexual abuse, including "an adult male's penis partially penetrating the vagina of a prepubescent female," and "an adult male masturbating and ejaculating into the mouth of a nude, prepubescent female." *Id.*, pp. 17-20, ¶¶ 18-25. Tellingly, the sub-section of Playpen that had the greatest number of postings was "Pre-teen" videos dubbed "Girls HC," where users viewed and shared hardcore pornographic images of pre-teen girls. *Id.*, p. 16, ¶ 14. Playpen also featured image and file hosting and a chat forum, all of which allowed users to upload links to child pornography. *Id.*, pp. 19-20, ¶¶ 23-25. As Judge Bryan observed in the *Michaud* case, the NIT warrant

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

affidavit demonstrated that Playpen was "unmistakably dedicated to child pornography." *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *5 (W.D. Wash. Jan. 28, 2016). And of course, all of this activity occurred before the FBI ever assumed control of Playpen.

The FBI thus had every reason to suspect Playpen users were actively engaged in the illegal viewing and sharing of child pornography. This applies with equal force to the user "Jimbox," the username ultimately linked to Lorente. Because this investigation was "focused on a category of persons [the government] had reason to believe were involved" in the crimes being investigated, the first two *Black* factors weigh heavily against any finding of outrageousness. *Black*, 733 F.3d at 304 (citing *United States v. Garza–Juarez*, 992 F.2d 896, 899-900 (9th Cir. 1993)).

B. The government played no role in creating the crime for which Lorente is being prosecuted.

The third *Black* factor assesses the government's role in creating the charged offense: that is, whether the government "proposed the criminal enterprise or merely attached itself to one that was already established and ongoing." *Black*, 733 F.3d at 305. This too weighs in the government's favor. The government did not create Playpen. It had been in operation for months when the government, with court authorization to investigate ongoing child sexual exploitation, seized the site in February 2015.[3] Nor, importantly, does the government bear any responsibility for Lorente's years-long interest in, and consumption of, child pornography. The only person to blame for the thousands of images of child pornography on Lorente's devices is Lorente himself. Even his connection to Playpen—he registered in November 2014—formed long before the FBI could have had any say in the matter. Dkt. 1, p. 4, ¶ 8.

[3] Lorente claims "the FBI exponentially increased the number of visitors to the site." Dkt. 30, p. 3. That is untrue. While it appears that there were more site visits during the two weeks FBI had administrative control over the site than estimates of earlier activity on the site, there is no reason to think the FBI's actions had anything to do with it. Nor does Lorente offer anything to support his claim that the FBI was the cause.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

This matters because courts have recognized that "outrageous" conduct is more likely to be found were the *government* fabricates the crime and then invites the *defendant* along for the ride. *See, e.g.*, *United States v. Mayer*, 503 F.3d 740, 754 (9th Cir. 2007) (finding no outrageous government conduct and noting that the defendant was the first to broach the subject of traveling internationally to have sex with boys). That is plainly not the case here.

C. The government did not encourage Lorente's participation in the criminal conduct.

The fourth *Black* factor assesses the extent to which the government encouraged the defendant to participate in the crimes at issue. *See Black*, 733 F.3d at 308. It did not. After all, Lorente admitted he had been viewing child pornography on a daily basis for fifteen years. Dkt. 1, p. 6, ¶ 16.

And, as noted above, Lorente joined Playpen on November 1, 2014, long before law enforcement seized it. Dkt. 1, p. 4, ¶ 6. Law enforcement had no direct contact with Lorente during the period when it had administrative control of the website, or beforehand. The most that can be said is that the government briefly operated a website that Lorente used to access child pornography. Lorente needed no encouragement from the government to do so.

D. The government's participation in Playpen was not responsible for Lorente's criminal conduct.

The fifth *Black* factor assesses the government's participation in the offense conduct by examining the duration, nature, and necessity of that participation. *See Black*, 733 F.3d at 308-09. With respect to duration, longer is more problematic. *See, e.g.*, *Greene*, 454 F.2d at 786 (finding outrageous government conduct where participation was of "extremely long duration," of between two-and-one-half and three-and-one-half years). With respect to the nature of the involvement, courts examine whether "the government acted as a partner in the criminal activity, or more as an observer of the defendant's criminal conduct." *Black*, 733 F.3d at 308. Lastly, there is the matter of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

necessity, which examines "whether the defendant[] would have had the technical expertise or resources necessary to commit such a crime without the government's intervention." *Id.* at 309 (emphasis in original). All three favor the government here.

First, the duration of the government's operation of Playpen was exceedingly brief: two weeks. Playpen itself operated for at least six months before that. Two weeks falls far short of the multi-year period deemed problematic by the Ninth Circuit in earlier cases. *See, e.g.*, *Greene*, 454 F.2d at 786.

Second, the nature of the government's involvement with Playpen was circumscribed. And the government's conduct falls far closer to the observer end of the spectrum. The FBI did not post any images, videos, or links to child pornography on the website. Playpen's users were responsible for that content.[4] While it is true that images, videos, and links posted by site users (both before the FBI assumed administrative control and after) generally remained available to site users for some limited period of time, for reasons explained below, removing all of that content would have jeopardized the investigation into the very users who possessed, distributed, and accessed it.

Lorente claims that law enforcement made no effort to curtail the redistribution of child pornography through Playpen or to determine whether images posted pertained to new, as opposed to known, images of child pornography. Dkt. 30, pp. 3, 7. Not so. While Playpen operated under FBI administrative control, FBI Special Agents monitored all site postings, chat messages, and private messages continuously to comply with Title III monitoring requirements and to assess and mitigate 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. Actions taken in any particular instance were tailored to the specific threat of harm.

---

[4] Lorente claims that actions of users who distributed child pornography through Playpen "require[d] the approval and technical assistance of whoever is operating the site." Dkt. 30, p. 2. That is wrong. In accordance with the site rules and guidelines, users posted messages containing child pornography images and/or links to such images or videos (along with necessary passwords) without any need for administrative approval or technical assistance.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Finally, no one could doubt that Lorente "had the technical expertise" and "resources" to commit the charged crimes "without the government's intervention." *Black*, 733 F.3d at 308. By his own admission, he had been consuming child pornography for years. Lorente, not the FBI, registered for an account with Playpen. And Lorente, not the FBI, downloaded thousands of images of child pornography.

In sum, the duration of the government's involvement was brief; its role was minimal; and Lorente committed these crimes all on his own. Thus, this factor, too, favors the government.

E. The government's conduct was necessary given the use of an anonymous network by Lorente and many others to conceal their locations and identities while advertising, sharing, and viewing child pornography.

The last and perhaps most important factor is the "need for the investigative technique that was used in light of the challenges of investigating and prosecuting the type of crime being investigated." *Black*, 733 F.3d at 309; *see also United States v. Emmert*, 829 F.2d 805, 812 (9th Cir. 1987) (holding $200,000 finder's fee inducement not outrageous because "large sums of money are common to narcotics enterprises and necessary to create a credible cover for undercover agents"); *United States v. Wiley*, 794 F.2d 514, 515 (9th Cir. 1986) (approving of the government's activation of a prison smuggling scheme given the "difficulties of penetrating contraband networks in prisons"); *Twigg*, 588 F.2d at 378 n.6 ("[I]n evaluating whether government conduct is outrageous, the court must consider the nature of the crime and the tools available to law enforcement agencies to combat it.").

There can be little doubt the government's investigative approach was necessary. As the government explained to the judges who authorized the NIT and the Title III and as those two judges apparently agreed, the brief, continued operation of Playpen in order to deploy the NIT was necessary to identify individuals actively sharing child pornography. Lorente and the other Playpen users used technology to conceal their identities and locations, not for fear of discovery of some lawful, if to many, distasteful,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

pursuit. To the contrary, they sought a safe haven where they could share child pornography without fear of law enforcement intervention. And but for the government's investigation, these offenders would have succeeded in remaining hidden. The government explained, in great detail, the problem it faced in identifying these criminals and why other investigative alternatives were simply not likely to succeed. Dkt. 48, Ex. 1, pp. 22-24, ¶¶ 29-32; Dkt. 48, Ex. 2, p. 26, ¶ 39 & pp. 30-31, ¶¶ 52-53.

Lorente claims that the government should have identified him and his fellow offenders differently. But his proposals, perhaps unsurprisingly, fails to account for the sort of advanced technical means that he and other Playpen users employed. As the government explained in the application for the Title III authorization: in order for the NIT to have an opportunity to work, members had to be able to continue to access the site, with as minimal an interruption in the operation of the site as possible, so as to not create suspicion that a law enforcement interdiction was taking place. Dkt. 48, Ex. 2, p. 37, ¶ 61. The affidavit specifically noted that interruptions in the service of the Playpen website, and others like it, would be a tip-off to suspects that law enforcement infiltration was taking place. *Id.*[5]

To be sure, agents considered seizing Playpen and removing it from existence immediately. *Id.*, p. 41, ¶ 72. Indisputably, doing so would have ended child pornography trafficking *on Playpen*. It should come as no surprise, however, that the problem extends far beyond Playpen.[6] Shutting down Playpen immediately would have squandered any hope of identifying and apprehending the offenders responsible for truly

---

[5] For the same reason, the investigative *alternatives* Lorente claims would have been preferable—*e.g.*, posting links with explicit titles that do not actually direct users to images, redirecting users to a spoofed site containing no child pornography content or links, rendering everything but the home page inaccessible, or sending users files that did not actually contain child pornography, Dkt 30, p. 8—would obviously have tipped users off to the fact of law enforcement infiltration and thus prevented law enforcement from identifying them.

[6] There are currently child pornography bulletin boards operating on the Tor network that are similar in structure and function to Playpen, 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 hidden services, the location of the computer servers hosting the websites, the locations and identities of their users who are perpetrating crimes against children, and their child victims, are currently unknown.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

abhorrent conduct. *Id.* It also would have frustrated agents' attempts to obtain information that could help identify and rescue child victims from ongoing abuse. *Id.* Accordingly, it was the judgment of law enforcement that the seizure and continued operation of Playpen for a limited period of time, paired with the deployment of a NIT and monitoring of user communications, was necessary and appropriate in order to identify Playpen users. *Id.* Two federal judges obviously agreed.

Stopping the unlawful possession and dissemination of child pornography, and rescuing children from ongoing abuse and exploitation, requires more than just shutting down a 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 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, all in an effort to identify those perpetrators. Undoubtedly, the decision whether to simply shut down a website like Playpen or to allow it to continue operating is a difficult one for law enforcement, given that users would continue to be able to post and access child pornography.[7] Here, that difficult decision, which was disclosed to two different judges, was amply justified by the particular facts of the investigation. Accordingly, the "investigative technique that was used" in this case was necessary given the "challenges of investigating and prosecuting the type of crime being investigated." *Black*, 733 F.2d at 309. Like the others, this last *Black* factor counsels against any finding of outrageousness.

---

[7] During the government's operation of Playpen, 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 herein. On March 4, 2015, it was determined that the balance of those factors weighed in favor of shutting down the website.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In sum, reasonable people may disagree about whether the benefits of any investigation undertaken outweigh its costs. That is not the question before the Court, however. The government took reasonable steps to address a significant challenge to its ability to investigate and prosecute serious crimes against children. And it did so after fully disclosing its intentions to two different judges. Whatever may be said about what the government did here, it did not act outrageously and certainly not in a matter that offends fundamental notions of fairness. Accordingly, Lorente's motion should be denied.

DATED this 7th day of March, 2016.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
Matthew P. Hampton
Andre M. Penalver
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
andre.penalver@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith Becker
Keith 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 March 7, 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(s) of record for the defendant(s).

s/Emily Miller
EMILY MILLER
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-2267
FAX: (206) 553-0755
E-mail: emily.miller@usdoj.gov

From: (b)(6); (b)(7)(C)
Sent: 5 May 2016 16:20:45 -0400
To: (b)(6); (b)(7)(C)
Subject: FW: Tor/NIT issues
Attachments: Dkt 49 MTD Respons(b)(6); pdf, R 41 Amend Order.pdf

---

From: (b)(6); (b)(7)(C)
Sent: Thursday, April 28, 2016 8:26:25 PM
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: FW: Tor/NIT issues

FYI cyber/electronic surveillance teams.

From: (b)(6); (b)(7)(C)
Sent: Thursday, April 28, 2016 7:39:34 PM
To: (b)(6); (b)(7)(C)
Subject: FW: Tor/NIT issues

FYSA.

Sent with Good (www.good.com)

(b)(6);
(202) 904(b)(6);
(b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: Thursday, April 28, 2016 7:16:53 PM
To: (b)(6); (b)(7)(C)
Subject: FW: Tor/NIT issues

See below from CEOS regarding Supreme court ruling today… LES

(b)(6);

From: Becker, Keith (b)(6); (b)(7)(C)
Sent: Thursday, April 28, 2016 6:26 PM
To: (b)(6); (b)(7)(C)
Cc:
Subject: Tor/NIT issues

(b)(6);

Good to meet you yesterday and thanks for taking the time to talk with me about criminal CE enforcement on Tor. To that end, wanted to give you an update that today, the Supreme Court approved an amendment to Rule 41 specifically permitting magistrates to issue warrants to

remotely search computers whose location is being concealed through technological means. I've attached the order and new rule, which will take effect December 1. (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

I've also attached one of the government's now-public filings in a WDWA case, a response to a defense motion to dismiss for alleged 'outrageous government conduct,' which the Court denied. (b)(5); (b)(7)(E)

(b)(5);

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

Look forward to continuing our great work with your unit in the future, and feel free to reach out anytime with questions. Thanks,

KB
Keith A. Becker
Acting Assistant Deputy Chief
Child Exploitation and Obscenity Section
(202) (b)(6); (b)(7)(C) (o)
(202) (c)

From: (b)(6); (b)(7)(C)
Sent: 21 Feb 2017 09:18:49 -0500
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: NIT case
Attachments: UNITED STATES OF AMERICA Appellant v Alex LEVIN Defendant-Appellee.pdf

Thought this might be of interest to everyone. Attached please find an amicus brief filed in a NIT case on appeal to the First Circuit.

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732(b)(6); (b)(7)((Desk)
202-536 (Cell)

2017 WL 633650 (C.A.1) (Appellate Brief)
United States Court of Appeals, First Circuit.

UNITED STATES OF AMERICA, Appellant,

v.

Alex LEVIN, Defendant-Appellee.

No. 16-1567.
February 10, 2017.

On Appeal from the United States District Court for the District of Massachusetts

Brief of Amicus Curiae Privacy International in Support of Defendant-Appellee and in Support of Affirmance of the Decision Below

Caroline Wilson Palow, 1st Cir. No. 1178172, Scarlet Kim, 1st Cir. No. 1177295, Privacy International, 62 Britton Street, London EC1M 5UY, United Kingdom, +44 (0) 20 3422 4321.

***II CORPORATE DISCLOSURE STATEMENT**

Pursuant to Federal Rule of Appellate Procedure 26.1, *amicus curiae* Privacy International certifies that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

***iii TABLE OF CONTENTS**

***v TABLE OF AUTHORITIES**

Cases

Statutes and Rules

Other Authorities

*1 STATEMENT OF INTEREST

Privacy International is a nonprofit, non-governmental organization based in London, the United Kingdom ("UK"), which defends the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into government and corporate surveillance with a focus on the technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States, the UK, and Europe, including the European Court of Human Rights. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect this right. It also strengthens the capacity of partner organizations in developing countries to identify and defend against threats to privacy.

Privacy International files this brief with the consent of all parties. [1]

*2 INTRODUCTION

The "network investigative technique" ("NIT") used by the government in this case is a novel, sophisticated and awesome power. Its novelty and sophistication make it difficult to grasp its operation. Yet, without this understanding, those tasked with authorizing and overseeing the NIT fail to comprehend the profoundly intrusive effect it can have on our electronic devices, upon which we increasingly depend to communicate with others, express our personal and political views, and store our most sensitive information. They may further fail to recognize the NIT's capability to affect connected devices anywhere in the world.

It seems the government would prefer to keep us in the dark. It uses vague and imprecise language, divorced from well-established technical vocabulary and concepts, to describe the NIT. By painting a picture of the NIT with such unintelligible brushstrokes, the government seeks to render a hazy impression of a tracking device. It asks us to imagine the NIT as a transmitter, like that we might affix to a vehicle, transposed to the digital realm. But the NIT is not a tracking device and therefore could not be authorized, as the government submits, pursuant to Federal Rule of Criminal Procedure 41(b)(4).

The NIT comprises distinct and intricate technical processes and components. Together, these processes and components operate to compromise the ***3** security of the devices of untold numbers of unknown individuals. They then perform a series of actions on the devices, including locating particular categories of information and then copying and sending that information from the devices to the government. Examined separately or as a whole, none of these processes or components constitute a tracking device within the meaning of Rule 41(b)(4).

From its warrant application to its brief before this Court, the government has also downplayed the international ramifications of using the NIT. We now know that the NIT infiltrated over 8,700 devices. Over 83% of these devices were located outside of the U.S., in 120 countries and territories. This outcome was entirely foreseeable to the government at the time of its warrant application.

The NIT warrant therefore authorized the government to undertake extraterritorial action. Well-established international law prohibits the government from undertaking law enforcement functions in other countries, without those countries' consent, which the government did not seek here. This principle is reflected in the warrant authority, which does not permit judges to authorize extraterritorial action. These legal constraints protect against the foreign relations risks incurred when the U.S. acts extraterritorially, risks that are particularly amplified when the U.S. interferes with the devices of thousands of individuals abroad.

***4** Where the government seeks to use new and complex technology to facilitate searches and seizures, that technology may not fit appropriately into existing categories of authorization. Incongruity should give the courts pause, for such technology may have unforeseen and powerful consequences, as revealed by a close and clear-eyed examination of the NIT. Here, the NIT failed to qualify as a tracking device or otherwise operate in a manner that would support the issuance of the NIT warrant. Its extraterritorial reach further renders the warrant invalid. For these reasons, this Court should uphold the decision below.

*5 ARGUMENT

I. THE DISTRICT COURT WAS CORRECT IN HOLDING THAT THE MAGISTRATE JUDGE LACKED AUTHORITY UNDER RULE 41(b)(4) TO ISSUE THE NIT WARRANT BECAUSE THE NIT IS NOT A "TRACKING DEVICE."

The government submits that Federal Rule of Criminal Procedure 41(b)(4) authorized the magistrate judge to issue the NIT warrant. Gov't Br. 23-32. Privacy International disagrees. According to a proper technical understanding of the NIT, the NIT cannot be characterized as a tracking device within the meaning of Rule 41(b)(4).

A. The government's characterization of the NIT as a "tracking device" is based on a technically misleading description of the NIT.

The government's description of the NIT obscures how the NIT works in practice. The NIT comprises multiple distinct processes, involving the use of distinct technical components. These processes render the NIT a technique to: [2]

***6** (1) send an "exploit" to devices in bulk;
(2) deploy the "exploit" to compromise the security of those devices; and

(3) run a "payload" to perform actions on the devices. [3]

Below, we unpack and explain each of these processes and components.

1. The NIT uses an "exploit" and a "payload."

An "exploit" takes advantage of a security "vulnerability" -- *i.e.* weakness or flaw -- in a computer system or application. [4] *See* Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 1, 22-23 (2014) ("A vulnerability is a weakness in a system ***7** that can potentially be manipulated by an unauthorized entity to allow exposure of some aspect of the system."). A physical world analogy to an exploit might be a trick to unlock a hotel safe unbeknownst to the user, such as by entering an override code. *See, e.g.*, Sam Biddle, *Can 000000 Secretly Open Your Hotel Safe?*, Gizmodo (Sept. 6, 2011), http://gizmodo.com/5837561/can-000000-secretly-open-your-hotel-safe.

An exploit, by taking advantage of a security vulnerability in a computer system or application, permits a "payload" to run. *See* Hennessey & Weaver, *supra* ("[T]he exploit opens a window in the owner's house that the owner believed was locked but which can be removed from the frame... and lets in the payload...."). Payloads are sometimes characterized as "malware," a term that may be more familiar to the Court. [5] Malware, a contraction of "malicious software," refers to computer code designed to perform actions on a system that, but for the malware, would not occur. *See* The Jargon File (Oct. 1, 2004), ***8** http://www.catb.org/jargon/index.html (entry for "malware"). [6] A "payload," in the computer security context, can refer to that part of malware that actually performs those actions. *See Terminology*, Malware Attribute Enumeration and Characterization, MITRE (Jan. 2, 2014), http://maec.mitre.org/about/terminology.html ("[A] malware's payload... is directly tied into the purpose behind the malware."). Extending the hotel safe analogy above, the exploit could be a method for unlocking the safe, while the payload could be any action taken once the safe is unlocked, including copying or stealing its contents.

2. The NIT sends an exploit to devices in bulk.

The first step of the NIT is to send an exploit to all devices visiting the Playpen website. *See* NIT Aff. ¶32 (G.Add:68). As the government's warrant application explains, "[i]n the normal course of operations, websites send content to visitors" and "[a] user's computer downloads that content and uses it to display web pages...." *Id.* ¶33 (G.Add:68). The FBI modified the code on the Playpen site itself so that when visitors requested content from the site, that content was "augment[ed]... with additional computer instructions." *Id.*; Motions Hearing Tr. at 76-77, *Michaud* (Jan. 22, 2016), ECF No. 203 (PI.Add:11-12) (Alfin test.) ("We ***9** configured the NIT to supplement the information being downloaded by the user with the NIT instructions."); *see also id.* at 112 (PI.Add:13) (Soghoian test.) ("[A] regular person just clicking around is not going to know there has been this new special code added to the web site."). What the government vaguely describes as "additional computer instructions," NIT Aff. ¶33 (G.Add:68); Gov't Br. 27, is, as clarified by one of its own experts, instructions to send an exploit. Levine Decl. ¶4 (PI.Add:24) ("Retrieving certain pages from the Playpen website resulted in the download of the FBI's exploit....").

This mode of delivery was bulk by nature, as every visitor to the targeted website would receive the exploit. The warrant application observed that, according to historical data about the Playpen site, it received over 1,500 unique users daily and over 11,000 unique users weekly. NIT Aff. ¶19 (G.Add:62). The application requested "authority to use the NIT, which will be deployed on the TARGET WEBSITE... to investigate any user or administrator who logs into the TARGET WEBSITE." *Id.* ¶32 (G.Add:68). The bulk nature of this technique is why it is commonly known as a "watering hole attack." *See* Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 Yale J.L. & Tech. 26, 41-42 (2016) (describing the FBI's use of watering hole attacks). Such attacks are designed to target unknown individuals in a group, by identifying websites (*i.e.*, watering ***10** holes) that their members frequent and installing code on those sites, which transmit an exploit to visiting devices. [7]

3. The NIT deploys the exploit to compromise the security of devices.

Once the exploit has been sent to a device, it takes advantage of a vulnerability in the Tor Browser program.[8] *See* Motions Hearing Tr. 114 ("[T]he NIT... bypassed the security controls within the Tor browser...."); *see also* Mozilla Motion 4 ("[T]he Exploit took advantage of a vulnerability in the browser software used by the Defendant."). The Tor Browser consists of a modified version of Mozilla's Firefox browser and Tor software. *What is Tor Browser?*, Tor, https://www.torproject.org/projects/torbrowser.html.en (last visited Feb. 3, 2017). Through the Tor Browser, users can connect to the Tor network, which protects their anonymity while using the internet. *See Tor: Overview*, Tor, ***11** https://www.torproject.org/about/overview.html.en (last visited Feb. 3, 2017). The Tor network also makes it possible for individuals to host websites, known as "hidden services," without revealing the location of the site. *See Tor: Hidden Service Protocol*, Tor, https://www.torproject.org/docs/hidden-services.html.en (last visited Feb. 3, 2017). A user can only visit a "hidden service" by using the Tor network; Playpen was one such hidden service.

In narrow terms, the exploit operated to circumvent the security protections of the Tor Browser, which normally prevents websites from determining certain identifying information of visitors. More broadly, however, by circumventing the security protections of the Tor Browser, the exploit compromised the security of the devices themselves.[9] *See* Motions Hearing Tr. 115-16 (PI.Add:14-15) ("Q. [T]he NIT bypasses security or overrides security features on the [target] computer.... A. That sounds right."); Miller Decl. ¶2 (PI.Add:16) ("[T]he NIT... compromised the security settings on [the defendant's] computer...."); Mozilla Motion 3 ("Mozilla has reason to believe that the Exploit... is an active ***12** vulnerability in its Firefox code base that could be used to compromise users and systems running the browser.").

4. The NIT runs a "payload" to perform actions on the compromised devices.

Once the exploit has compromised the security of a device, the NIT runs a payload.[10] *See* Levine Decl. ¶4 (PI.Add:24) ("Much like a tool to open a locked door to a house, the purpose of the exploit was to allow for the execution of the payload program on a defendant's computer."). Here, the payload was designed in part to locate certain information on the device to assist "in identifying the user's computer, its location, and the user of the computer." NIT Aff. ¶34 (G.Add:68-69) (listing the information sought by the government); Levine Decl. ¶4 (PI.Add:24) ("The payload program queried a defendant's computers for certain information...."). The payload was further designed to copy and transmit that information from the device to the government.[11] *See* Alfin Decl. ¶11 (PI.Add:6) (describing the NIT ***13** as having "gathered specific information... and transmitted that information to government controlled computers").

B. According to a proper technical understanding of the NIT, the NIT cannot be characterized as a "tracking device" within the meaning of Rule 41(b)(4).

The definition of "tracking device," as used in Rule 41, is "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b); Fed. R. Crim. P. 41(a)(2)(e) (incorporating this definition). The government explains that, "applied to older technologies, the Rule contemplates that a tracking device may be a mechanical tool used to track the movement of a tangible object," such as a transmitter affixed to a vehicle. Gov't Br. 27. Translated to "newer technologies," the government submits that "the Rule envisions that a tracking device may be an electronic device used to track the movement of information -- *e.g.*, computer instructions embedded in digital content traveling on data highways, like the NIT in this case." *Id.*

The NIT is not a single "electronic device" or even a single "set of 'computer instructions.' " The very first step of the NIT reveals it comprises multiple sets of "computer instructions": the "instructions" on the modified Playpen site to send the exploit to devices in bulk as well as the exploit and the payload themselves. Furthermore, the NIT, taken as a

whole, does not operate to "track the movement of information." Rather, its primary functions are to ***14** compromise the security of many unknown devices in bulk in order to perform a series of actions on those devices.

The tracking device analogy also collapses if we separately examine each of the processes and components that make up the NIT. The government suggests that the first step of the NIT -- the watering hole attack -- served a tracking function, by "follow[ing] illegal child pornography content requested by a user who accessed Playpen." Gov't Br. 28. But the watering hole attack neither follows nor tracks information. Rather, it *sends an exploit* to visitors to the Playpen website. *See* Motions Hearing Tr. 112 (PI.Add:13) ("[T]he website tells the web browser, 'Do this.' The code is downloaded to... the Tor browser... [a]nd it is only when the instructions are received by the Tor browser... that they are run on that computer ...."). And even if we were to analogize the watering hole attack to the "installation" of a tracking device, it would require contemplating installation on thousands of vehicles simultaneously, whose locations and owners are unknown. [12]

In any event, neither the exploit nor the payload can be fairly characterized as a "tracking device." The exploit operates exclusively to compromise the security of devices so as to permit the payload to run. The payload then performs a series of ***15** actions -- locating, copying, and sending information from those devices to the government. A tracking device, according to the government's own analysis, performs only the last step. Gov't Br. 27 ("Similar to a transmitter affixed to an automobile that is programmed to send location-enabling signals (like GPS coordinates)..., the NIT... was designed to send location-enabling information... back to a government-controlled computer....").

Even to the extent that the final step of the payload -- transmission of information to the government -- overlaps with how a tracking device operates, critical differences remain. Unlike a tracking device, the payload does not transmit information related to the *movement* of anything. *See* 18 U.S.C. § 3117(b) (defining "tracking device," as used in Rule 41, as "an electronic... device which permits the tracking of the *movement* of a person or object") (emphasis added). Nor is the payload even confined to transmitting information related solely to the location of devices. Rather, the payload was explicitly designed to locate, copy, and transmit multiple categories of information -- such as the device's "host name" and active operating system username -- beyond those that would simply assist in identifying the location of the devices. *See* NIT Aff. ¶34 (G.Add.:69).

For the reasons set forth above, the NIT cannot properly be characterized as a "tracking device" within the meaning of Rule 41(b)(4).

***16 II. THE NIT WARRANT IS INVALID BECAUSE IT AUTHORIZED EXTRATERRITORIAL SEARCHES AND SEIZURES.**

The government explains that "[t]he FBI used the NIT to identify the IP addresses of hundreds of Playpen users located across the country," but noticeably fails to mention the extraterritorial reach of its operation. Gov't Br. 8. In separate criminal proceedings arising out of the government's execution of the NIT warrant, the government recently disclosed that the NIT affected thousands of devices located in 120 countries and territories. Evidentiary Hearing Tr. at 18, *Tippens* (Nov. 1, 2016), ECF No. 103 (PI.Add:20). Specifically, the NIT returned 8,713 IP addresses, 7,281 (over 83%) of which were foreign. *Id.* at 39 (PI.Add:22).

Much of the litigation around the country challenging the validity of the NIT warrant, including in this case, has centered around the domestic jurisdictional limitations imposed by Rule 41. *See* Gov't Br. 17-19 (citing cases). But absent from this debate is a consideration of the extraterritorial jurisdictional limitations on the warrant authority. Below, Privacy International discusses the international and domestic legal bases for these limitations. Privacy International then describes some of the foreign relations implications of authorizing the NIT warrant.

A. International law prohibits unilateral extraterritorial searches and seizures.

International law subjects a state to limitations on its authority to exercise extraterritorial jurisdiction. *Restatement (Third) of Foreign Relations Law in the* ***17** *United States* § 401 (Am. Law Inst. 1987). A state exercises what is called enforcement jurisdiction when it undertakes some form of executive action. [13] In the criminal context, the U.S. exercises enforcement jurisdiction when its law enforcement "effect[s] legal process coercively, such as to arrest someone, or to undertake searches and seizures." Robert Cryer et al., *An Introduction to International Criminal Law and Procedure* 44 (2d ed. 2010).

Enforcement jurisdiction is generally constrained by territory. Thus, "[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state...." *Restatement (Third), supra*, at § 432(2); *see also* Int'l Bar Ass'n, *Report of the Task Force on Extraterritorial Jurisdiction* 9-10 (2009) ("[A] state cannot investigate a crime, arrest a suspect, or enforce its judgment or judicial processes in another state's territory without the latter state's permission.") (citing SS Lotus (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7); Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.) 2002 I.C.J. 3 ¶¶4, 49, 54 (Feb. 14)). These restrictions apply to remote searches and seizures of devices located abroad. *See* American Bar Ass'n, *International Guide to Combating Cybercrime* 154 (2002) (criticizing ***18** unilateral cross-border data searches as "inevitably allow[ing] one state to transgress upon another state's sovereignty by searching and seizing property... that is physically located within that second state's territory"); Patricia L. Bellia, *Chasing Bits across Borders*, U. Chi. Legal F. 35, 77-80 (2001) (explaining why "the customary international law rule against one state conducting investigative activities in another state's territory provides a strong basis for states to object to remote cross-**border searches** of data within their territory").

B. Rule 41 does not authorize extraterritorial searches and seizures.

The warrant authority reflects the "territorial-based limits" of enforcement jurisdiction:

> The overarching rule is that the judiciary's warrant authority is territorially limited. After all, under well-accepted principles of international law, State A can exercise law enforcement actions in State B only if State B consents. As a result, judges are presumed to lack authority to unilaterally authorize extraterritorial searches and seizures.

Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 354 (2015) (citing, *inter alia, Restatement (Third), supra*, at § 432(2); James Crawford, *Brownlie's Principles of Public International Law* 478-49 (8th ed. 2012)). Thus, Rule 41 generally limits search and seizure authorization to persons or property located within the district in which the magistrate judge sits. *See* Fed. R. Crim. P. 41(b)(1)-(2), (4). And "[e]ven in those limited situations... in which judges are permitted to issue warrants authorizing out-of-district searches or seizures, such ***19** warrants are still widely understood to be subject to territorial-based limitations." Daskal, *supra*, at 355; *see also id.* (noting that the "instances [under Rule 41(b)(5)] in which magistrate judges are explicitly authorized to issue a warrant with extraterritorial reach... extend to locations where the United States already exerts significant (if not exclusive) regulatory authority, thereby avoiding potential conflict with foreign jurisdictions and maintaining respect for other nations' sovereign authority to enforce the law"). The government's own commentary on its proposed amendment to Rule 41 -- which now permits out-of-district searches where the location of "the media or information... has been concealed through technological means" -- observes that "[i]n light of the presumption against international extraterritorial application... this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries." Letter from Mythili Raman, Acting Assistant Att'y Gen., to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 2 (Sept. 18, 2013) (SA:4) ("Raman Letter"); *see also infra* note 14. The government therefore acknowledges, at least in principle, that Rule 41 does not -- and did not prior to its amendment on December 1, 2016 -- authorize courts to issue warrants that authorize extraterritorial searches and seizures using techniques such as the NIT.

***20 C. The magistrate judge lacked authority to issue the NIT warrant because it authorized extraterritorial searches and seizures.**

By authorizing the NIT warrant, the magistrate judge authorized the government to conduct extraterritorial searches and seizures. [14] The NIT's extraterritorial reach was foreseeable at the time the government made its warrant application. The government submitted that "using the Tor network... obscure[e]s a user's true location" and accordingly explained the NIT's purpose as "reveal[ing] to the government... information that may assist in identifying the user's computer, *its location*, and the user of the computer." NIT Aff. ¶¶8, 34 (G.Add:11, 68-69) (emphasis added); *see also supra* 11 (explaining that as a "hidden service," the Playpen website required visitors to connect to it using the Tor network). If the physical location of a device is cloaked, it may be anywhere in the world. Moreover, at the time of the government's warrant application, over 80% of Tor users were connecting to the network from outside the U.S. *Tor Metrics*, Tor, https://metrics.torproject.org/userstats-relay-table.html?start =2015-02- ***21** 01&end=2015-02-28 (last visited Feb. 3, 2017) (refining search of "Top-10 countries by relay users" to the month of February 2015). Accordingly, the NIT warrant is invalid because it authorized extraterritorial searches and seizures.

D. The foreign relations risks posed by unilateral extraterritorial searches and seizures further counseled against authorization of the NIT warrant.

The magistrate judge's authorization of the NIT warrant has potentially profound foreign relations implications. As discussed above, well-established principles of international law prohibit unilateral extraterritorial searches and seizures. In accordance with these principles, the U.S. traditionally relies on consent-based mechanisms for obtaining evidence located extraterritorially. [15] The principal mechanism is a Mutual Legal Assistance Treaty ("MLAT"), a bilateral agreement containing procedures for obtaining and providing assistance in criminal matters. [16] *See* T. Markus Funk, Fed. Judicial Ctr., *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges* 5 (2014). Law enforcement agencies may also participate directly in various other types of cooperative arrangements. [17]

***22** Consent-based mechanisms help avoid jurisdictional -- and thereby diplomatic -- conflict between states. [18] *See* Int'l Bar Ass'n, *supra*, at 30. The government itself recognizes and warns its personnel against these risks. The U.S. Attorney's Criminal Resource Manual accordingly instructs:

The other nation may regard an effort by an American investigator or prosecutor to investigate a crime or gather evidence within its borders as a violation of sovereignty. Even such seemingly innocuous acts as a telephone call, a letter, or an unauthorized visit to a witness overseas may fall within this stricture. A violation of sovereignty can generate diplomatic protests and result in denial of access to the evidence or even the arrest of the agent or Assistant United States Attorney who acts overseas. The solution is usually to invoke the aid of the foreign sovereign in obtaining the evidence.

Dep't of Justice, U.S. Attorney's Manual, *Criminal Resources Manual* § 267. The DOJ's Computer Crime and Intellectual Property Section extends this precaution to the digital realm, warning: "[S]ome countries may object to attempts by U.S. law enforcement to access computers located within their borders. Although the search may seem domestic to a U.S. law enforcement officer executing the search in the United States..., other countries may view matters differently." Computer Crime & Intellectual Prop. Section, Dep't of Justice, *Searching and Seizing* ***23** *Computers and Obtaining Electronic Evidence in Criminal Investigations* 85 (2009) (SA:41).

Here, the government unilaterally deployed the NIT, which poses particular risks. *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, U.C. Hastings Legal Res. Paper No. 170 24 (2016) ("A review of applicable treaties and diplomatic communications reveals that no state has consented to the United

States' launch of cross-border network investigative techniques."). If the FBI were to conduct a physical search or seizure abroad, the nature of the extraterritorial action would be clear from the outset. But in the digital realm, "incidents will probably involve a publicly ambiguous set of facts" because "[m]alicious computer code or actions in cyberspace... are opaque to public view, technically very complex and likely to emerge piecemeal." Matthew C. Waxman, *Self Defense Force Against Cyber Attacks*, 89 Int'l L. Stud. 109, 119 (2013); *see also* Susan W. Brenner, *Cyber-threats and the Limits of Bureaucratic Control*, 14 Minn. J.L. Sci. & Tech. 137, 171 (2013) ("[W]hen our activities migrate into cyberspace, it becomes correspondingly difficult for nation-states to ascertain the nature of the threats they confront."). As a result, other states may mischaracterize the NIT and similar techniques, heightening the risk of diplomatic conflict.

***24** In addition, as the above excerpt from the DOJ's *Criminal Resources Manual* notes, the use of the NIT may violate the domestic law of other states. *See supra* 22. Reversing the scenario, foreign deployment of a NIT-like technique against U.S. devices in order to locate, copy and transmit information would violate U.S. law. *See, e.g.*, Computer Crime & Intellectual Prop. Section, Dep't of Justice, *Prosecuting Computer Crimes Manual* 16-19 (2010) (describing intentional access to a computer without authorisation to obtain information as a violation of 18 U.S.C. § 1030(a)(2), a provision of the Computer Fraud and Abuse Act). The violation of foreign laws carries with it the risk of foreign prosecution. For instance, in 2002, Russia's Federal Security Service ("FSB") filed criminal charges against an FBI agent for remotely accessing and copying data from a Russian server. [19] Brunker, *supra; see also United States v. Gorshkov*, No. 00-cr-550, 2001 WL 1024026 (W.D. Wash., May 23, 2001).

The government suggests that if it is not permitted to seek authorization for the NIT pursuant to Rule 41, it may have to "resort[] to warrantless searches justified by claims of exigency." Gov't Br. 25. To the extent that the government ***25** claims that its extraterritorial action requires no authorization at all, such a position violates well-established international law and practice, which condemns the unilateral exercise of extraterritorial searches and seizures. Privacy International further counsels against a conclusion that there is no role for judicial authorization to play in the context of extraterritorial searches and seizures. In an era in which more and more of our data -- emails, texts, phone calls, documents and photos -- seamlessly and arbitrarily travels across borders or sits abroad, we may need to fundamentally reconsider traditional doctrines of extraterritoriality as they apply to law enforcement action. This exercise requires thoughtful and careful study, well beyond the scope of this brief, as to how best to balance privacy rights, investigative efficacy and national sovereignty in the digital era. Rule 41, however, is not sufficient on its own to authorize extraterritorial searches and seizures.

***26 CONCLUSION**

For the reasons set forth above, *amicus curiae* Privacy International respectfully requests that this Court affirm the ruling below.

Dated February 10, 2017

Respectfully submitted,

/s/ Caroline Wilson Palow

Caroline Wilson Palow

1st Cir. No. 1178172

Scarlet Kim

1st Cir. No. 1177295

Privacy International

62 Britton Street

London EC1M 5UY

United Kingdom

+44 (0) 20 3422 4321

caroline@privacyinternational.org

Appendix not available.

Footnotes

1 Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), counsel for *amicus curiae* state that no counsel for a party authored this brief in whole or in part, and no person other than *amicus curiae* or its counsel made a monetary contribution to its preparation or submission.

2 Privacy International relies primarily on expert declarations and testimony in other criminal proceedings arising out of the government's execution of the NIT warrant to describe the NIT. These statements were elicited in conjunction with motions to compel discovery regarding the NIT pursuant to Federal Rule of Criminal Procedure 16(d). *See, e.g., United States v. Matish*, No. 16-cr-16 (E.D. Va.); *United States v. Michaud*, No. 15-cr-5351 (W.D. Wa.); *United States v. Tippens*, No. 16-cr-5110 (W.D. Wa.). They currently constitute the most detailed technical information in the public domain about how the NIT operates. We rely on representations from experts for both the government, *see* Decl. of Brian Levine, *Tippens* (Sept. 22, 2016), ECF No. 58-1 (PI.Add:23); Decl. of Special Agent Daniel Alfin, *Matish* (June 1, 2016), ECF No. 74-1 (PI.Add:4), and various defendants, *see* Decl. of Christopher Soghoian, *Matish* (June 10, 2016), ECF No. 83-1 (PI.Add:1); Decl. of Matthew Miller, *Michaud* (May 9, 2016), ECF No. 191-1 (PI.Add:16), and note where these representations diverge from each other. The government's addendum is cited as "G.Add," the supplemental appendix is cited as "SA" and Privacy International's addendum is cited as "PI.Add."

3 Privacy International does not address aspects of the NIT that do not directly pertain to whether it can be properly characterized as a tracking device. These aspects include its generation of a "unique identifier" to distinguish information collected from different devices and a "server component," which refers to the FBI system for receiving, recording and storing information transmitted from devices. *See* Alfin Decl. ¶¶18-19, 24-25 (PI.Add:7-8).

4 Experts for the government do not dispute that it used an exploit, but have not taken a clear position on whether the exploit constitutes part of the NIT itself. *Compare* Levine Decl. ¶4 (PI.Add:24) ("[M]y understanding of the overall process used by the FBI is as follows. A defendant's computer connected using the Tor network to the Playpen website.... Retrieving certain pages from the Playpen website resulted in the download of the FBI's exploit and payload programs.") *with* Alfin Decl. ¶11 (PI.Add:6) ("[A]n 'exploit' allowed the FBI to deliver a set of instructions -- the NIT -- to Matish's computer.... The NIT instructions and results have been provided to the defense for review; the 'exploit' has not."). Experts for defendants in NIT cases as well as scholars following this wave of litigation agree that the exploit constitutes a component of the NIT. *See, e.g.*, Miller Decl. ¶¶2-3 (PI.Add:16-17) (agreeing with another expert that there are "four major components" to the NIT and proceeding to discuss the "exploit" as one of those components); Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, Lawfare (July 28, 2016), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques (describing the "exploit" as one of "a number of distinct components" comprising the NIT).

5 Experts for the government do not dispute that it used a payload. *See, e.g.* Levine Decl. ¶4 (PI.Add:24); Alfin Decl. ¶7 (PI.Add:5). The government has however, in certain circumstances, objected to the use of the term "malware" to describe any part of the NIT. *See, e.g.*, Gov't's Surreply to Defendant's Motion to Compel Discovery at 11-13, *Matish* (June 1, 2016), ECF No. 74. Nevertheless, computer security experts have used this term to describe the NIT. *See* Soghoian Decl. ¶¶5-12 (PI.Add:2-3); Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired (Aug. 5, 2014)

https://www.wired.com/2014/08/operation_torpedo/ ("From the perspective of experts in computer security and privacy, the NIT is malware, pure and simple.") (describing prior FBI operations employing NITs).

6 The Jargon File is a glossary of computer programming terms, originally compiled by early computer programming communities, which has also been published as *The New Hacker's Dictionary* (Eric S. Raymond ed., MIT Press, 1996) (1983).

7 The term "watering hole attack" is commonly used in the computer security field, even though the government has objected to its use to describe any part of the NIT. *See* Soghoian Decl. ¶10 n.9 (PI.Add:3) ("The D [OJ] has taken the position that bulk delivery of NITs in operations like Playpen are not watering hole attacks.... [T]he D[OJ] and the technical community do not see eye to eye."); *see also* Brian Krebs, *Espionage Hackers Target 'Watering Hole' Sites*, Krebs on Security (Sept. 25, 2012), https://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites/(describing watering hole attacks).

8 The government has not denied that the exploit takes advantage of a vulnerability in the Tor Browser program but has not disclosed the exploit itself. Accordingly, the exact nature of the exploit remains unclear, which may account for why it has been described as both code and command. *Compare* Alfin Decl. ¶11 (PI.Add:6) ("As used here, a computer 'exploit' consists of lines of code that are able to take advantage of a software vulnerability.") *with* Mozilla's Motion to Intervene or Appear as *Amicus Curiae* at 4, *Michaud* (May 11, 2016), ECF No. 195 ("[T]he exploit is not malware or a program, but a command...."); *see generally* Bellovin et al., *supra*, at 23 (explaining that an exploit "can be a software program, or a set of commands or actions").

9 Experts for the government do not dispute that the exploit compromised the security of devices, but dispute that the exploit made "*fundamental* changes or alterations to a computer system or to disable its security firewall" (while admitting that these scenarios are "theoretically possible"). Alfin Decl. ¶¶11, 14 (PI.Add:6) (emphasis added); Levine Decl. ¶6(b) (PI.Add:25) (stating "there is no evidence to support" the hypothesis that "an FBI exploit or payload made *permanent* changes to the security settings or any other settings of the defendants' computers") (emphasis added).

10 In part because the exact nature of the exploit remains unclear, *see supra* note 8, the details of how the payload was delivered to devices are also murky. A "dropper" is a component of malware that typically "installs the payload on the target system." Bellovin et. al, *supra*, at 24. However, a dropper can be "single stage, a program that executes... as a direct result of a successful exploit," which "carries a hidden instance of the payload," or "it can be multi-stage, executing on the target system, but downloading... the payload... from a remote server." *Id.*

11 The "actual IP address," one of the categories of information sought by the government was not technically seized from the devices themselves. Rather, it appears that as the data copied from the devices was transmitted to the government, the actual IP address attached itself to that data and was thereby revealed to the government. The technical details of this aspect of the NIT are beyond the scope of this brief.

12 The government further argues that the NIT "was installed in the Eastern District of Virginia, as required by Rule 41(b)(4)." Gov't Brief 29. Because Privacy International disputes that the NIT is a tracking device, it does not address this argument. It notes, however, that the defendant-appellee's computer never physically entered or left the Eastern District of Virginia. *See* Amended Memorandum & Order 14 (G.Add:14).

13 A state can exercise three types of jurisdiction: (1) prescriptive ("*i.e.* to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things"), (2) adjudicative ("*i.e.* to subject persons or things to the process of its courts"), or (3) enforcement ("*i.e.* to induce or compel compliance... with its laws or regulations"). *Restatement (Third), supra*, at § 401.

14 The government accepts that an extraterritorial search or seizure occurs if the device from which information is searched or seized is located abroad. On December 1, 2016, amendments proposed by the DOJ to Rule 41 went into effect, authorizing magistrate judges "to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if... the district where the media or information is located has been concealed through technological means." Fed. R. Civ. P. 41(b)(6). In a letter to the Rules Committee, the DOJ explained that "[i]n light of the presumption against international extraterritorial application... this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries." Raman Letter, *supra*, at 2 (SA:2). The government therefore submits that "the search of electronic storage media located" abroad constitutes an extraterritorial search.

15 For an overview of the range of consent-based mechanisms, see Michael Abbell, *Obtaining Evidence Abroad in Criminal Cases* (2010).

16 The U.S. currently has MLATs in force with over 70 countries. Charles Doyle, Cong. Research Serv., *Extraterritorial Application of American Criminal Law* 23 (2016). MLATs are negotiated by the State Department and implemented by the DOJ's Office of International Affairs. Dep't of State, 7 *Foreign Affairs Manual* § 962.1.

17 The U.S. is, for example, a member of the International Criminal Police Organization (Interpol), which enables countries to route requests for law enforcement assistance through its network. Abbell, *supra*, at 9 & n.47. Moreover, federal law enforcement agencies, such as the FBI, may transmit requests for investigative assistance through their liaisons or attachés stationed at embassies and consulates abroad. *Id.* at 10 & nn.50-51.

18 Jurisdiction, in this sense, is "a proxy for state power," defining the "legal relationship" between "the state to other sovereigns." Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 Harv. Int'l L.J. 121, 126 (2007).

19 Russia's reaction can be understood as an assertion of sovereignty. *See* Mike Brunker, *FBI agent charged with hacking*, NBC News (Aug. 15, 2002), http://www.nbcnews.com/id/3078784 (citing FSB sources "describing the criminal complaint as an effort to restore traditional law enforcement borders" and quoting one such source as stating, "[i]f the Russian hackers [who were the subjects of the FBI investigation] are sentenced on the basis of information obtained by the Americans through hacking, that will imply the future ability of U.S. secret services to use illegal methods in the collection of information in Russia and other countries").

End of Document

From: (b)(6);
Sent: 29 Sep 2017 10:55:15 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: In the news... Dream Market Admin

I think it's a good point—I'll add it to the "Sharing" slide. Thanks!

(b)(6); (b)(7)(C)
Associate Legal Advisor
CLS | HSILD | OPLA | ICE
202-732-(b)(6); desk)
202-731-(b)(7) mobile)

From: (b)(6); (b)(7)(C)
Sent: Friday, September 29, 2017 10:28 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: FW: In the news... Dream Market Admin

FYI. (b)(5)

(b)(5)

(b)(6); (b)(7)(C)
Deputy Chief
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6); (Desk)
202-536-(b)(7)(Cell)

From: (b)(6); (b)(7)(C)
Sent: Wednesday, September 27, 2017 7:05 AM
To: (b)(6); (b)(7)(C)
Subject: In the news... Dream Market Admin

Good morning,
How goes it?
Here is yet another reminder of the importance of sealing affidavits and other documents or at least limiting details that aren't required for PC. This news story highlights several specific details from a DEA case against a Marketplace admin. It also notes that critical information was discovered through a border search.

http://www.miamiherald.com/news/nation-world/article175557206.html
I know y'all don't get tons of opportunities to train AUSAs, but when you do, could you please share the importance of sealing documents?
Have a great day!

(b)(6); (b)(7)(C)

HSI C3
504-609-(b)(6); (b)(7)(C)

Page 44

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 45

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 46

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 47

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 48

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 49

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 50

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 51

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 52

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 53

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 54

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 55

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 56

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 57

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

From: (b)(6); (b)(7)(C)
Sent: 5 Apr 2018 17:18:51 -0400
To: (b)(6); (b)(7)(C)
Subject: USSS
Attachments: Government Use of Malware

I chatted with (b)(6); at the USSS. (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(6); (b)(7)(C)
Associate Legal Advisor
OPLA, HSI Law Division, Criminal Law Section
U.S. Immigration and Customs Enforcement

202 (b)(6); (b)(7)(C) desk
202 cell
(b)(6); (b)(7)(C) @dhs.gov

From: (b)(6); (b)(7)(C) (LEG)
Sent: 5 Apr 2018 18:23:45 +0000
To: (b)(6); (b)(7)(C) @dhs.gov
Subject: Government Use of Malware

Hello Ms (b)(6); (b)(7)(C)

I'm an attorney with the Secret Service Criminal Investigative Division, and I recently received a question from the field about (b)(5); (b)(7)(E)
(b)(5); (b)(7)(E) Have you ever addressed a similar issue at HSI, and if so would you be free for a quick phone call to discuss? We're still at a very conceptual level.

Thanks,
Steve Giballa
Attorney Advisor
U.S. Secret Service
202 (b)(6); (b)(7)(C)

From: (b)(6);
Sent: 29 Mar 2017 13:40:40 -0400
To: (b)(6); (b)(7)(C)
Cc:
Subject: CFU and CCU Meeting Notes

(b)(6);

I wanted to give you some notes from my meetings yesterday with CFU and CCU. Overall they went well and I'm glad I was able to sit down and meet to everyone. We mainly discussed encryption (CFU) and intrusion (CCU), but CFU also brought up some other issues, all of which, I believe, are currently being addressed by CLS.

CFU:

(b)(5); (b)(7)(E)

CCU:

(b)(5); (b)(7)(E)

Hope this helps.

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section|Homeland Security Investigations Law Division

Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (desk)
202-731- (mobile)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 25 Jan 2018 15:00:54 -0500
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: Fourth Circuit upholds use of FBI's NIT

http://www.ca4.uscourts.gov/opinions/174299.P.pdf

The court didn't reach the Fourth Amendment question of whether the FBI's warrant was valid, but lets in evidence under the good-faith exception. The court joins the 1st, 8th, and 10th Circuits in permitting evidence gathered using the FBI's Tor exploit.

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (office)
202-731-[illegible] (mobile)
(b)(6); (b)(7)(C)

Page 63

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 64

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 65

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 66

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 67

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 68

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(A) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

From: (b)(6); (b)(7)(C)
Sent: 16 May 2017 12:32:16 -0400
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: FW: NIT Software

Thought others on the team might like to see this NIT discussion. Tracks with my last understanding of this issue.

From: (b)(6);
Sent: Tuesday, May 16, 2017 7:54 AM
To: (b)(6); #ces-Child Exploitation Program; (b)(6); (b)(7)(C)
Subject: RE: NIT Software

All,

(b)(5); (b)(7)(E)

That being said, I am checking a few other LE partners to see if they have anything that might assist but we don't have anything at C3 right now.

(b)(6);

From: (b)(6); (b)(7)(C)
Sent: Monday, May 15, 2017 11:01 PM
To: #ces-Child Exploitation Program; (b)(6); (b)(7)(C)
Subject: FW: NIT Software

(b)(5); (b)(7)(E)

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(6); (b)(7)(C)
Date: Monday, May 15, 2017, 7:56 PM
To: (b)(6); (b)(7)(C)
Subject: NIT Software

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

The USAO case # is (b)(6); (b)(7)(A); (b)(7)(C); (b)(7)(E)

(b)(5); (b)(7)(E)

Thanks

(b)(6);

From: (b)(6); (b)(7)(C)
Sent: 23 Aug 2016 15:20:23 -0400
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: Just FYI; U.S. v. Matish; interesting decision in multiple contexts

***U.S. v. Matish*, 2016 WL 3545776 (EDVA; 7/28/2016)**
This is an interesting case in the context of Fourth Amendment / suppression and cybercrime / child pornography I thought I would flag. To really delve into the technical aspects you'll need a full read (especially to understand the network investigative technique (NIT) employed by the FBI in this case and some of the collateral factors / arguments).
(b)(5)

(b)(5)

The *Matish* Op. further states:

> "FBI agents who exploit a vulnerability in an online network do not violate the Fourth Amendment. Just as the area into which the officer in Carter peered—an apartment—usually is afforded Fourth Amendment protection, a computer afforded Fourth Amendment protection in other circumstances is not protected from Government actors who take advantage of an easily broken system to peer into a user's computer. People who traverse the Internet ordinarily understand the risk associated with doing so. "

(b)(5)

(b)(5)

(b)(5)

(b)(5)

As the Supreme Court has emphasized again and again in recent years, the suppression of evidence is not the appropriate remedy for every violation of the Fourth Amendment. Herring v. United States, 555 U.S. 135, 140 (2009) (citing Illinois v. Gates, 462 U.S. 213, 222 (1983)). "Each time the exclusionary rule is applied it exacts a substantial societal cost for the vindication of Fourth Amendment rights." Rakas v. Illinois, 439 U.S. 128, 137 (1978). Accordingly, the exclusionary rule is the "last resort" for the courts and should be the "first impulse." Utah v. Strieff,

136 S. Ct. 2056, 2061 (2016) (quoting Hudson v. Michigan, 547 U.S. 586, 591 (2006). Suppression is only appropriate when the benefits of suppression outweigh its costs. Herring, 555 U.S. at 141 (citing United States v. Leon, 468 U.S. 897, 910 (1984)).

United States v. Eure (2016 WL 4059663 at *5) (EDVA July 28, 2016).

(b)(5)

(b)(6); (b)(7)(C)
Associate Legal Advisor
U.S. Immigration and Customs Enforcement
Office of the Principal Legal Advisor
Homeland Security Investigations Law Division
Criminal Law Section
(202) 732-(b)(6) (office)
(202) 308- (iPhone)
(b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)
Sent: 28 Sep 2016 08:40:42 -0400
To: (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)
Subject: NIT article

https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/?utm_term=.f79bd5bf51d1

Interesting article from our boy (b)(6); about the NIT used in the Playpen cases. I don't (b)(5) (b)(5) but the article is a good summary of the issues implicated by NITs.

(b)(6); (b)(7)(C)
Associate Legal Advisor
Criminal Law Section
Homeland Security Investigations Law Division
Office of the Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-(b)(6) (Desk)
202-536-(b)(7) (Cell)