

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

3 FEDERAL RULES OF CRIMINAL PROCEDURE

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

5 FEDERAL RULES OF CRIMINAL PROCEDURE

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

7 FEDERAL RULES OF CRIMINAL PROCEDURE

(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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

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

15 In contrast, there are numerous reported decisions where courts have declined to
16 dismiss an indictment in the face of alleged outrageous conduct—even in cases involving
17 so-called “reverse stings”—where the government initiates the criminal conduct by
18 inventing a fictitious criminal scenario and then prosecutes a defendant who attempts to
19 participate in it. *See, e.g., United States v. Pedrin*, 797 F.3d 792, 794 (9th Cir. 2015)
20 (affirming finding of no outrageous government conduct where an “undercover agent
21 pose[d] as a disgruntled drug courier with knowledge about a stash house . . . containing
22 a large amount of cocaine,” suggested “to targets of the reverse sting that they join forces,
23 rob the house, and split the proceeds,” and then “arrested and charged [them] with
24 conspiracy” once the targets took “steps to rob the fictional house”); *Black*, 733 F.3d at
25 302 (affirming finding of no outrageous government conduct in similar fictional stash-
26 house sting operation planned by government agent because, when “presented with the
27 fictitious stash house robbery proposal [the targets] . . . readily and actively” participated
28 in the criminal activity “as willing participants”). The standard is all the higher where, as

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

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

8 (1) known criminal characteristics of the defendant[]; (2) individualized
 9 suspicion of the defendant[]; (3) the government’s role in creating the crime
 10 of conviction; (4) the government’s encouragement of the defendant[] to
 11 commit the offense conduct; (5) the nature of the government’s
 12 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.

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

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

20 It is easy to argue, and, my gosh, we hear it in all kinds of cases, that the
 21 other side’s position is outrageous. Well, you know, that’s a high standard.
 22 From the standpoint of one who stands between the defendant and the
 23 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.

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

25
 26
 27
 28 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.

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

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

5 The FBI thus had every reason to suspect Playpen users were actively engaged in
 6 the illegal viewing and sharing of child pornography. This applies with equal force to the
 7 user “Jimbox,” the username ultimately linked to Lorente. Because this investigation was
 8 “focused on a category of persons [the government] had reason to believe were involved”
 9 in the crimes being investigated, the first two *Black* factors weigh heavily against any
 10 finding of outrageousness. *Black*, 733 F.3d at 304 (citing *United States v. Garza–Juarez*,
 11 992 F.2d 896, 899-900 (9th Cir. 1993)).

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

14 The third *Black* factor assesses the government’s role in creating the charged
 15 offense: that is, whether the government “proposed the criminal enterprise or merely
 16 attached itself to one that was already established and ongoing.” *Black*, 733 F.3d at 305.
 17 This too weighs in the government’s favor. The government did not create Playpen. It
 18 had been in operation for months when the government, with court authorization to
 19 investigate ongoing child sexual exploitation, seized the site in February 2015.³ Nor,
 20 importantly, does the government bear any responsibility for Lorente’s years-long
 21 interest in, and consumption of, child pornography. The only person to blame for the
 22 thousands of images of child pornography on Lorente’s devices is Lorente himself. Even
 23 his connection to Playpen—he registered in November 2014—formed long before the
 24 FBI could have had any say in the matter. Dkt. 1, p. 4, ¶ 8.

25
 26
 27 ³ Lorente claims “the FBI exponentially increased the number of visitors to the site.” Dkt. 30, p. 3. That is untrue.
 28 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.

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

7 **C. The government did not encourage Lorente’s participation in the**
8 **criminal conduct.**

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

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

19 **D. The government’s participation in Playpen was not responsible for**
20 **Lorente’s criminal conduct.**

21 The fifth *Black* factor assesses the government’s participation in the offense
22 conduct by examining the duration, nature, and necessity of that participation. *See Black*,
23 733 F.3d at 308-09. With respect to duration, longer is more problematic. *See, e.g.,*
24 *Greene*, 454 F.2d at 786 (finding outrageous government conduct where participation
25 was of “extremely long duration,” of between two-and-one-half and three-and-one-half
26 years). With respect to the nature of the involvement, courts examine whether “the
27 government acted as a partner in the criminal activity, or more as an observer of the
28 defendant’s criminal conduct.” *Black*, 733 F.3d at 308. Lastly, there is the matter of

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

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

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

16 Lorente claims that law enforcement made no effort to curtail the redistribution of
17 child pornography through Playpen or to determine whether images posted pertained to
18 new, as opposed to known, images of child pornography. Dkt. 30, pp. 3, 7. Not so.
19 While Playpen operated under FBI administrative control, FBI Special Agents monitored
20 all site postings, chat messages, and private messages continuously to comply with Title
21 III monitoring requirements and to assess and mitigate risk of imminent harm to children.
22 In the event that FBI Special Agents perceived a risk of imminent harm to a child, agents
23 took actions to mitigate that risk and immediately forwarded available identifying
24 information, including NIT results, to the appropriate FBI office. Actions taken in any
25 particular instance were tailored to the specific threat of harm.

26
27 ⁴ Lorente claims that actions of users who distributed child pornography through Playpen “require[d] the approval
28 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.

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

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

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

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

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

1 | pursuit. To the contrary, they sought a safe haven where they could share child
2 | pornography without fear of law enforcement intervention. And but for the government's
3 | investigation, these offenders would have succeeded in remaining hidden. The
4 | government explained, in great detail, the problem it faced in identifying these criminals
5 | and why other investigative alternatives were simply not likely to succeed. Dkt. 48, Ex.
6 | 1, pp. 22-24, ¶¶ 29-32; Dkt. 48, Ex. 2, p. 26, ¶ 39 & pp. 30-31, ¶¶ 52-53.

7 | Lorente claims that the government should have identified him and his fellow
8 | offenders differently. But his proposals, perhaps unsurprisingly, fails to account for the
9 | sort of advanced technical means that he and other Playpen users employed. As the
10 | government explained in the application for the Title III authorization: in order for the
11 | NIT to have an opportunity to work, members had to be able to continue to access the
12 | site, with as minimal an interruption in the operation of the site as possible, so as to not
13 | create suspicion that a law enforcement interdiction was taking place. Dkt. 48, Ex. 2, p.
14 | 37, ¶ 61. The affidavit specifically noted that interruptions in the service of the Playpen
15 | website, and others like it, would be a tip-off to suspects that law enforcement infiltration
16 | was taking place. *Id.*⁵

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

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

28 | 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.

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

7 | Stopping the unlawful possession and dissemination of child pornography, and
8 | rescuing children from ongoing abuse and exploitation, requires more than just shutting
9 | down a facility through which such materials are disseminated. Law enforcement must
10 | identify and apprehend the perpetrators. Here, the FBI briefly assumed administrative
11 | control over an existing facility through which users were already posting and accessing
12 | child pornography to deploy a court-authorized investigative technique and engage in
13 | court-authorized monitoring of user communications, which were necessitated by the
14 | particular anonymizing technology deployed by the users of the site, all in an effort to
15 | identify those perpetrators. Undoubtedly, the decision whether to simply shut down a
16 | website like Playpen or to allow it to continue operating is a difficult one for law
17 | enforcement, given that users would continue to be able to post and access child
18 | pornography.⁷ Here, that difficult decision, which was disclosed to two different judges,
19 | was amply justified by the particular facts of the investigation. Accordingly, the
20 | "investigative technique that was used" in this case was necessary given the "challenges
21 | of investigating and prosecuting the type of crime being investigated." *Black*, 733 F.2d at
22 | 309. Like the others, this last *Black* factor counsels against any finding of
23 | outrageousness.

24 |
25 | _____
26 | ⁷ During the government's operation of Playpen, regular meetings were held to discuss the status of the investigation
27 | and identification of site users and assess whether the site should continue to operate, based upon a balancing of
28 | 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.

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

9 DATED this 7th day of March, 2016.

10 Respectfully submitted,

11 ANNETTE L. HAYES
12 United States Attorney

STEVEN J. GROCKI
Chief

13
14 /s/ Matthew P. Hampton

15 Matthew P. Hampton
16 Andre M. Penalver
17 Assistant United States Attorney
18 1201 Pacific Avenue, Suite 700
19 Tacoma, Washington 98402
20 Telephone: (253) 428-3800
21 Fax: (253) 428-3826
22 E-mail: matthew.hampton@usdoj.gov
23 andre.penalver@usdoj.gov

/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 Responses (b)(6); (b)(7)(C).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: (b)(6); (b)(7)(C)
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)(7)(E)

(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) (b)(7)(C) (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); (Desk)
202-536-(b)(7)(Cell)

*** Warning *** Attorney/Client Privilege *** Attorney Work Product ***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

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**

TABLE OF AUTHORITIES	v
STATEMENT OF INTEREST	1
INTRODUCTION	2
ARGUMENT	5
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.”	5
A. The government's characterization of the NIT as a “tracking device” is based on a technically misleading description of the NIT	5
1. The NIT uses an “exploit” and a “payload.”	6
2. The NIT sends an exploit to devices in bulk	8
3. The NIT deploys the exploit to compromise the security of devices	10
4. The NIT runs a “payload” to perform actions on the compromised devices	12
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)	13
II. THE NIT WARRANT IS INVALID BECAUSE IT AUTHORIZED EXTRATERRITORIAL SEARCHES AND SEIZURES	16
A. International law prohibits unilateral extraterritorial searches and seizures... ..	16
B. Rule 41 does not authorize extraterritorial searches and seizures	18
C. The magistrate judge lacked authority to issue the NIT warrant because it authorized extraterritorial searches and seizures	20
*iv D. The foreign relations risks posed by unilateral extraterritorial searches and seizures further counseled against authorization of the NIT warrant	21
CONCLUSION	26
CERTIFICATE OF COMPLIANCE	27
CERTIFICATE OF SERVICE	28
ADDENDUM	

***v TABLE OF AUTHORITIES**

Cases

Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.) 2002 I.C.J. 3 (Feb. 14) 17
 SS Lotus (Fr. v. Tur.) 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7) 17

Statutes and Rules

18 U.S.C. § 1030(a)(2) 24
 18 U.S.C. § 3117(b) 13, 15
 Fed. R. Crim. P. 41 (2011) *passim*

Other Authorities

Michael Abbell, *Obtaining Evidence Abroad in Criminal Cases* (2010) 21, 22
 American Bar Ass'n, *International Guide to Combating Cybercrime* (2002) . 17
 Patricia L. Bellia, *Chasing Bits across Borders*, U. Chi. Legal F. 35 (2001) . 18
 Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 1 (2014) 6, 10, 12
 Sam Biddle, *Can 000000 Secretly Open Your Hotel Safe?*, Gizmodo (Sept. 6, 2011), <http://gizmodo.com/5837561/can-000000-secretly-open-your-hotel-safe> 7
 Susan W. Brenner, *Cyber-threats and the Limits of Bureaucratic Control*, 14 Minn. J.L. Sci. & Tech. 137 (2013) 23
 Mike Bruner, *FBI agent charged with hacking*, NBC News (Aug. 15, 2002), <http://www.nbcnews.com/id/3078784> 24
 *vi Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 Harv. Int'l L.J. 121 (2007) 22
 Computer Crime & Intellectual Prop. Section, Dep't of Justice, *Prosecuting Computer Crimes Manual* (2010) 24
 Computer Crime & Intellectual Prop. Section, Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) 22
 James Crawford, *Brownlie's Principles of Public International Law* (8th ed. 2012) 18
 Robert Cryer et al., *An Introduction to International Criminal Law and Procedure* 44 (2d ed. 2010) 17
 Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326 (2015) ... 18, 19
 Dep't of Justice, U.S. Attorney's Manual, Criminal Resources Manual 22, 24
 Dep't of State, Foreign Affairs Manual 21
 Charles Doyle, Cong. Research Serv., *Extraterritorial Application of American Criminal Law* (2016) 21
 T. Markus Funk, Fed. Judicial Ctr., *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges* (2014) 21
 Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, U.C. Hastings Legal Res. Paper No. 170 (2016) 23
 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> 6, 7
 Int'l Bar Ass'n, *Report of the Task Force on Extraterritorial Jurisdiction* (2009) 17, 22
 *vii The Jargon File (Oct. 1 2004), <http://www.catb.org/jargon/index.html> 7
 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/> 10

Zach Lerner, <i>A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure</i> , 18 Yale J.L. & Tech. 26 (2016)	9
Letter from Mythili Raman, Acting Assistant Att’y Gen., Criminal Div., Dep’t of Justice, to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules (Sept. 18, 2013)	19, 20
<i>Terminology</i> , Malware Attribute Enumeration and Characterization, MITRE (Jan. 2, 2014), http://maec.mitre.org/about/terminology.html	8
<i>The New Hacker's Dictionary</i> (Eric S. Raymond ed., MIT Press, 1996) (1983)	8
Kevin Poulsen, <i>Visit the Wrong Website, and the FBI Could End Up in Your Computer</i> , Wired, Aug. 5, 2014, https://www.wired.com/2014/08/operation_torpedo/	7
<i>Restatement (Third) of Foreign Relations Law in the United States</i> (Am. Law Inst. 1987)	16, 17, 18
<i>See Tor: Overview</i> , Tor, https://www.torproject.org/about/overview.html.en (last visited Feb. 3, 2017)	10
<i>Tor: Hidden Service Protocol</i> , Tor, https://www.torproject.org/docs/hidden-services.html.en (last visited Feb. 3, 2017)	11
<i>Tor Metrics</i> , Tor, https://metrics.torproject.org/userstats-relay-table.html?start=2015-02-01&end=2015-02-28 (last visited Feb. 3, 2017)	20
<i>What is Tor Browser?</i> , Tor, https://www.torproject.org/projects/torbrowser.html.en (last visited Feb. 3, 2017)	10
*viii Matthew C. Waxman, <i>Self Defense Force Against Cyber Attacks</i> , 89 Int’l L. Stud. 109 (2013)	23

***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

