UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, vs. DAVID TIPPENS, Defendant.	Docket No. CR16-5110RJB Tacoma, Washington November 1, 2016
UNITED STATES OF AMERICA, Plaintiff, vs. GERALD LESAN, Defendant.	Docket No. CR15-387RJB
UNITED STATES OF AMERICA, Plaintiff, vs. BRUCE LORENTE, Defendant.	Docket No. CR15-274RJB

TRANSCRIPT OF EVIDENTIARY HEARING CONTINUED
BEFORE THE HONORABLE ROBERT J. BRYAN
SENIOR UNITED STATES DISTRICT COURT JUDGE

Court Reporter: Teri Hendrix
Union Station Courthouse, Rm 3130
1717 Pacific Avenue
Tacoma, Washington 98402
(253) 882-3831

Proceedings recorded by mechanical stenography, transcript produced by Reporter on computer.

APPEARANCES:

For the Plaintiff:	**MATTHEW HAMPTON** **Assistant United States Attorney** **700 Stewart Street, Suite 5220** **Seattle, Washington 98101-1271**
	KEITH BECKER **U.S. Department of Justice** **1400 New York Avenue NW, 6th Floor** **Washington, DC 20530**
For Defendant Tippens:	**COLIN FIEMAN** **Office of the Public Defender** **1331 Broadway, Suite 400** **Tacoma, Washington 98402**
For Defendant Lesan:	**ROBERT W. GOLDSMITH** **Law Office of Robert W. Goldsmith** **702 2nd Avenue** **Seattle, Washington 98104**
For Defendant Lorente:	**MOHAMMAD ALI HAMOUDI** **Office of the Public Defender** **1601 5th Avenue, Suite 700** **Seattle, Washington 98101**

Tuesday, November 1, 2016 - 9:30 a.m.

(Defendants present.)

THE CLERK: THE CLERK: All rise. Court is again in session, the Honorable Robert J. Bryan presiding.

THE COURT: Please be seated. Good morning. I have this morning reread your briefing on the motion to suppress. I guess what I want to say is, you don't have to argue everything that's in your brief. I want to hear what you have to say, but give me some credit for having spent some time and effort on this and having read the briefs.

How much time do you get in the Supreme Court? Not long.

MR. FIEMAN: Well, on important cases, usually about an hour, and I certainly tend to be much less than that, Your Honor. My only caveat is that I need to learn to speak more slowly at the same time.

THE COURT: I had a hard time hearing what you said. I have to read it on real-time. Anyway, I am quite willing to hear whatever you want to say about these matters. I know that judges all over the country now have gone in different directions on different issues within these cases, and I guess I wanted to tell you something that should be obvious, and that is that I am interested in Ninth Circuit law when there is Ninth Circuit law. Law from other circuits is not what I have to follow if there is clear Ninth Circuit law.

Anyway, let's proceed.

MR. FIEMAN: Your Honor, I assume you want to hear from me first since I am the movant. Thank you.

Your Honor, I just wanted to begin briefly by updating you -- and I hope I am speaking closely enough to the microphone -- on just some of the appeal status.

I wanted to say one thing on the threshold matter about the status on appeal because you mentioned Ninth Circuit law, and what appears to be emerging is a pattern of the government delaying or avoiding appellate review that is desperately needed in these cases in a timely manner. We should have had the *Michaud* briefs, our reply brief, already submitted at this point awaiting oral argument. The government, over my objection, has requested another 60 days and has informed me that the solicitor general has not even approved the appeal at this point.

The *Arterbury* case, where there was suppression on magistrate grounds, the government dismissed its notice of appeal in that case last week. The *Barber* case, which we discussed, deals with the magistrate court issues at the motion to suppress, page 14. The government dismissed its appeal. And I believe in the *Levin* case out of Boston, there were three requests for continuances.

So in the threshold matter, I believe if the government is confident in its arguments, particularly in the Ninth Circuit, we should be getting more appellate guidance in a more timely

manner, and that is not happening.

Now Your Honor, we left off yesterday talking about a little bit about the governmental misconduct, and I just want to --

THE COURT: If you run that up about three or four inches, you will be speaking into the mike.

MR. FIEMAN: So I went back and looked at 3509. It's not a discovery statute. The second provision was added later. It's a general prohibition on the reproduction of child pornography, and subsection 2 was added because the government had taken such a strict view of discovery that they were not even giving it to defense attorneys. So it is a general prohibition.

I start there because what we've seen in this case, if you look at all the circumstances, is a consistent position on the part of the government that the rules don't apply to them in this investigation.

3509(m), they say does not apply. Rule 41 does not apply. The Magistrate's Act does not apply. The prohibition on foreign searches doesn't apply. The Rule 16 discovery rules don't apply because we are saying we have a law enforcement exemption. The Ninth Circuit's explicit duty of candor from *Comprehensive Drug Testing* does not apply. We did not tell Magistrate Judge Buchanan about it being a global warrant. We never told Magistrate Judge Buchanan we were going to be

actively distributing child pornography from Playpen.

We included a misleading description of the home page which, regardless of how that happened -- and clearly, the government was aware of it -- they never submitted a corrected application or did anything to make the home page conform to the description in the warrant.

We have the face of the warrant itself, Your Honor. That warrant itself, the first page where it talks about the place to be searched, in the Eastern District of Virginia, period. That was drafted -- submitted as a draft warrant by a prosecutor in Virginia, and I am going to be talking about how they are saying now, even though it says Eastern District of Virginia, period, on the face of the warrant, that doesn't bind us either. And then they turn around and say, you know what, Your Honor, we acted in good faith and you should ignore every one of those things.

So let me first talk about suppression or, I guess more technically, exclusion based on the discovery issues. The status of discovery at this point, Your Honor, is unchanged since *Michaud*, and we've been pursuing some sort of accommodation or middle ground with the government for over a year. We put our first discovery request in for the NIT components in September of 2014.

So Mr. Tsyrklevich describes very succinctly in his original declaration, which we have attached to docket 35, the

four components that make up an NIT. It's called a technique because -- rather than just code or malware -- because they all work in conjunction. It's like you can't drive the car if you say well, I have got the engine, but I don't need the wheels. They all work in conjunction.

So it's unchanged. We still do not have the exploit component; that's unchanged since *Michaud*. We don't have the server component, unchanged. We don't have the complete payload, unchanged.

And I want to point out here, Your Honor, that I do think there was one particular part where Professor Levine was not candid. If you look at his testimony and his declaration, he initially informed the Court that he had reviewed the payload, our payload. As we learned on cross-examination, he said he only looked at certain portions that were "human-readable." Well, that is exactly the same situation that Mr. Tsyrklevich was in when this whole discovery process started to become more serious.

You may remember from his declaration that he could not really determine what the payload did because of the incomplete information. Mr. Levine says that it's not hard to figure out what a human unreadable code does, yet he didn't even bother to do it himself. And in fact, it can't be done, according to Mr. Tsyrklevich's declaration, and all the defense experts, including Professor Reyzin from Boston who

reviewed all of them, without all the components working in conjunction.

Now, Your Honor, what's also remarkable here is we talked a little bit along the way -- I know Your Honor is familiar with the Nebraska cases, Operation Torpedo, the *Cottom* case. Everything that was available was turned over in that case, and if it was material then, how is it not material now?

Well, I understand that Your Honor is privy to information about why this is so sensitive, but what I am going to be talking about is essentially where we ended up in *Michaud*. The government has a right to withhold sensitive information because you have made that determination, but that does not answer the question of whether our clients can get a fair trial or whether there needs to be some remedial or balancing sanction in order to make this consistent with due process.

So I want to talk a little bit -- point you to the law that you are asking for, Your Honor -- and start with *Soto-Zuniga,* which is a remarkable decision that came down recently, Your Honor, because it essentially tracked your analysis in *Michaud*, relying on the same cases of *Hernandez-Meza*, *Budziak*, the same law that we laid out, and essentially summarized it and emphatically reaffirmed it.

So as we have on the monitor, Your Honor, just a few basic points. The Ninth Circuit has said "materiality is a low threshold." In addition they say, "The test is not whether

the discovery is admissible at trial, but whether it may assist in formulating a defense, or even just lead to additional admissible evidence." And this is the really, I think, remarkable outer limit that the Ninth Circuit has laid out because it really defines -- it makes it simple.

"Information is material even if it simply causes a defendant to abandon a planned defense and take a different path," and this is not a heavy burden for us to meet. It is material as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or merely assisting with impeachment or rebuttal.

Your Honor, I don't think there is any reasonable dispute or question about the materiality of this evidence, because think about it in these terms. The government has taken three runs at this. We had the initial motion to compel on *Michaud* and all the reconsideration litigation, and now the third time around they have Professor Levine, one expert against our six.

Now, let's assume for the moment that Professor Levine had actually looked at all the components, which he did not do. Let's assume that he was not relying on Agent Aflin's declarations about what he thinks he did or did not do, and let's assume that Agent Alfin actually looked at this stuff, which he didn't. So it's like an elaborate game of telephone. But even if all that could be credible, those issues are,

first of all, for a jury. And secondly, even if he is right, and we look at this stuff and it leads us to abandon all the defenses that we are formulating in terms of the exploits, damage and changes to our client's computers, it would still be material in discovery. So we are very far beyond this threshold.

Your Honor, you will recall -- and I just want to show how far along we are. And again, following up on your question about focussing on Ninth Circuit law, let me direct Your Honor to a case that we have cited, and that is the *Budziak* case, at 697 F.3d 1105. And I have the relevant quotes on the screen.

This case is interesting. You may remember I started with Professor Levine, asking him if he was a specialist in something particularly called peer-to-peer software and asked him some basic questions about, you know, whether an expert should be able to look at that software. Now, peer-to-peer software, Your Honor, is fairly commonplace. It frankly compares to the technical issues that we are dealing with in this case, very simple. Most of it is off the shelf.

Now, in *Budziak* where the issue was peer-to-peer software, they held as follows: "A party seeking to impeach the reliability of computer evidence" -- which is exactly what we are trying to do here, Your Honor -- "should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data have performed

their tasks accurately."

We are not required and should not, in fact, take the government's mere assurances, especially when nobody, including Agent Alfin, has actually seen this data. And then really this is the kicker, the second quote, this is where they come down: "It is incomprehensible that the prosecution should tender a witness to state the results of a computer's operations without having the program available for defense scrutiny and cross-examination." And this is a case with simple software, nothing like the complicated, sophisticated and novel components that we are dealing with here.

Your Honor, in *Michaud*, you summed it up in your oral findings, and I will quote -- this is from docket 31.1 of the Tippens case, the transcript we supplied: "The discovery that the defense has requested is central to the case, it's central to the search warrant that was issued, it's central to the proof that might be offered at trial, it is the background for the whole case."

None of that has changed. The discovery issues are exactly the same now, Your Honor. In *Soto-Zuniga*, finally, you must recall that the Ninth Circuit ultimately ruled that it was an abuse of discretion for the trial judge not to order discovery. In the very same case, Your Honor, the court recognized that much of that information was sensitive and potentially subject to law enforcement exemptions. The Ninth

Circuit said ultimately it makes no difference, you've got to fashion appropriate protective orders, or if those are not sufficient, they remanded with an instruction that the government has a window of opportunity -- I am quoting -- either to elect between accommodating discovery requests with protective orders, security measures or dismiss it. And anything else was an abuse of discretion.

Now, Your Honor, that ruling is in fact grounded in a Supreme Court decision, *United States v. Jencks*, 353 U.S. 657, and I have that up on the screen, too. In *Jencks*, the issue came down to what we have here. There are rare cases where there is an unbridgeable conflict between the government's election or right to keep certain information exempt or secret and a defendant's right to effective representation and a fair trial.

In *Jencks*, this is where they came down -- and I have the quote on the screen, Your Honor: "The rationale of the criminal cases is that, since the government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense."

This is what they ultimately ruled, and *Soto-Zuniga* tracks in its entire analysis.

The second quote from pages 671 to 672 is that, "The

criminal action must be dismissed when the government, on the ground of privilege, elects not to comply with an order to produce." Here's the final thing, Your Honor, and the one thing that I think is very important is where this decision rests. The Supreme Court made a very interesting point. This actually is not even a decision that a trial judge should be forced to make, although ultimately they will have to under Rule 16 if the government chooses not to.

But what the Supreme Court said is that it's actually the government's burden, because they have the overarching interest of fairness in upholding the Constitution. It is the government's burden "not to be shifted to the trial judge, to decide whether the public prejudice of allowing the alleged crime to go unpunished is greater than that attendant upon disclosure." That's their duty, and they won't fulfill it in this case, which is why we've made the motion to exclude and suppress on discovery grounds.

Now, Your Honor, let's just talk about how central this evidence is. Let's go back to the amicus brief that Mozilla submitted in *Michaud*, and it's cited in our exclusion motion. Here, this is essentially a third party; they have no stake in this case. Mozilla is a key technical component of the Tor network because they make the browser that is most commonly used, so they have extraordinary technical knowledge about the Tor network; it's really on the size of Google. They also

make a Firefox browser for general use. Here's what they concluded -- not even in reference to our experts, just in terms of the limited disclosures that the government had made through Agent Alfin: "The information contained in the declaration of Agent Alfin suggests that the government exploited" -- using the exploit -- "the very type of vulnerability that would allow third parties to obtain total control of an unsuspecting computer."

That goes to the heart of a big part of our defense in this case, not even the Fourth Amendment issues and all the essential cross-examination issues at trial, all the chain of custody issues. But I mean, that's a big part of our defense right there, and that's never been disputed by any government expert.

So let me continue. That tracks exactly what Mr. Tsyrklevich told this Court a year ago, and I am talking specifically about the exploit right now. I know Professor Levine initially tried to carve out the exploit as somehow separate and apart from the rest of the components, but I will get to that in a moment.

But Mr. Tsyrklevich, on page 3 of his declaration, talks specifically about the exploit, and he talks about how it works in conjunction with the payload, and he's unable to make a determination about what happened to our clients' computers without the code. Now, that's not just the defense expert

saying that. It's essentially the government, too.

Now, this is Agent Alfin's testimony from October 11th -- and I had this up earlier with Professor Levine because he ultimately had to agree with it. So they agree that exploit may make fundamental changes or alterations to a computer system or disable a security firewall.

Now, I know that the government keeps saying that that didn't happen in this case. That's what they have been saying from the beginning, and we have no basis to believe it or challenge it when we get to trial or in pretrial motions.

Now, in fact, interestingly, Professor Levine ultimately ended up agreeing not only with me but with Aflin's statements about what exploits can do. He also agreed with Professor Miller. Professor Miller and Shawn Kasal and Vlad Tsyrklevich, unlike Professor Levine, have all worked on prior NIT cases, including in Miller and Kasal's case, Operation Torpedo.

Professor Miller submitted to this Court -- and all of our witnesses have been available to the government, Your Honor; they have not requested to cross-examine them or challenge their declarations, apart from Professor Levine. But Professor Miller informed this Court that the alterations caused by exploits can cause a loss or alteration of data or alter any of the settings, and Professor Levine agreed with that.

Ultimately, Professor Levine, as you can see from paragraph 9, ultimately said that all of his information about the exploit came solely from Agent Alfin and Agent Alfin has not seen it. Then, of course, we have the server component that's missing and the incomplete payload. And then as well, Your Honor, let me talk about just the flow of the data itself, and I have the diagram up on the screen.

We now know, which was not clear at the time of the *Michaud* ruling, if I recall correctly, that a big part of this communication with these target computers was not even encrypted. The part from the exit relay on the Tor network to the government's server, which is listed as "destination," was not encrypted.

Professor Levine spent a long time talking about the "to" and "from" addresses, the packets. And the problem is that you cannot tell what's in the package from the address, and more importantly, it's more really like an evidence room. Assuming the package gets there, if you have the evidence room unlocked, everything is misnumbered, the data that they are putting out -- going to try to put out at trial -- we have no idea if it matches up because we have not seen the server component.

So we are in exactly the same position that we were in *Michaud*, and even if there was a legitimate dispute on the core issues between the experts, that's a trial issue. We

cannot even cross-examine the government effectively on most of this evidence without the discovery.

Let me now turn, if I may -- unless you have any questions about the discovery and exclusion on that ground, Your Honor -- to the Fourth Amendment issues. Let me back up for one second and talk specifically about the Fourth Amendment context. Your Honor, I really believe that these cases represent something of a crossroads, where the courts really must choose how they are going to exercise oversight in highly-technical cases and deal with the ever more sophisticated and secret technology that we are going to be seeing.

You know, a lot of this is really hard to grasp. We talk about Russia hacking into servers, Yahoo cooperating with the FBI to read the email content of customers. We've talked to the Court at various times about the Stingray cases where the government did not disclose that they were using technology. There's litigation going on in California right now where they still won't disclose aspects of that.

At some point, we are going to be losing control of our Constitution's machinery. If there isn't oversight that's meaningful by the courts, which involves candor on the part of the government and the ability of defense counsel to challenge the presumptions and representations of the government's experts, and ultimately the courts, to ensure that the

government is not slipping things by magistrate judges or exceeding their powers without comprehensive judicial oversight. So will the courts require the FBI to be candid and transparent going forward? Will the government be required to follow the rules even if they disagree with them because we live by the rule of law?

When it comes to law enforcement, are we going to start saying the ends justify the means, no matter the collateral consequences or the revictimization that's involved? These are core principles of our judicial system that I believe are seriously implicated in this case. If there aren't some bright lines laid down, then the technology and the secrecy is going to simply get away from us.

Now, what do we know now, Your Honor, six months after the *Michaud* ruling. Every time Your Honor grants a discovery request and we get new information, it's like -- to use an appropriate metaphor, like peeling an onion. There's just another layer of fact there that we did not know about. I mean, we did not know this was a truly global warrant before. There are 120 countries and territories listed outside the United States that the FBI hacked into, and they also hacked into something called a "satellite provider." So now we are into outer space as well.

Now, they did that -- and we've submitted this as an exhibit in our supplemental discovery. They did this in spite

of the fact that -- and I have this on the screen, Your Honor -- the U.S. Department of Justice assuring the Federal Rules Committee. And I will read from the letter that I put up: "In light of the presumption against international extraterritorial applications and consistent with the existing language of Rule 41" -- and I have a typo there because I had to type it out -- "this amendment does not purport to authorize courts to issue warrants that authorize searches in foreign countries." That's even with the proposed amendment, let alone the existing one.

Did the government disclose to Magistrate Judge Buchanan that this was a global warrant when she had never issued such a thing? So Your Honor, let's talk about the Magistrate's Act. It's interesting that the government has very, very little to say about it in its pleadings. They do not seriously dispute that it is jurisdictional.

Congress made the decision about the limitations in terms of the warrant issue and spoke of it, under Rule 41, which is incorporated by statute and then also under the Magistrate's Act. Every case -- although the courts have been all over the maps in terms of the remedies that may be appropriate here, every case where the defendants have raised the Magistrate's Act issue -- and I think there are six -- the courts have found they violated, and only one found that there was good faith, which I will get to shortly.

The act is jurisdictional. It cannot be expanded. It cannot be changed. It's just like 3509(m). You don't get to distribute child pornography when Congress has expressly prohibited it. You don't get to ignore the plain letter of the law and then claim reasonable minds may differ about whether you should follow it.

Now, Your Honor, the Court previously found that the Rule 41 violations -- we didn't get into the Magistrate's Act issues, but now moving to the Rule 41 violations, the Court found that there was no -- there was no provision in Rule 41 that allowed for a global one, but we didn't know it was quite global at that point, but apparently the Court made those findings, and they stand here.

But more importantly, I don't think there can be any serious dispute, knowing what we know now, that first of all, we've satisfied everything the Ninth Circuit requires to show that this was not a technical violation, this was a fundamental violation. And fundamental violations, Your Honor, we do submit, require suppression. So apart from the Magistrate's Act, which its own grounds for suppression, in Rule 41, we know this was clearly prejudicial, the first prong, because all we have to show is that the search would not have occurred without the violation. Well, they couldn't be searching in Washington with a Virginia warrant unless they violated Rule 41.

The privacy interest at stake here isn't the IP address or MAC address, it's the fact that they went into a personal computer in our clients' homes. We briefed that extensively, *Riley* and *Jones* and *Kyllo.* The government very predictably did not address any of that Supreme Court authority in its briefing, so this is dispositive. The privacy interest is the location of the search.

And by the way, I mentioned the MAC address. Let me back up one second on that. One of the things that we also learned last Wednesday -- thanks to your discovery order -- is that the NITs did not also always capture the MAC addresses. You will notice that in Exhibit 1 of the supplemental submission in the letter. MAC addresses were not always captured. This exploit was programmed to reliably and consistently capture the IP and MAC addresses.

So we already know, just from that very limited disclosure, that the exploit, the NIT, did not operate as intended in every single case. That alone is a red flag of either a programming error or bugs or inconsistent deployment possibly depending on the type of operating system that was on the computer, possibly depending on the type of security settings, all sorts of potential issues because the government has now disclosed that it did not even act consistently as instructed.

So, Your Honor, we know this is prejudicial because of the

search location. We know this is deliberate. I mean --

THE COURT: Just a second. Let me go back here. I am curious about the relationship with the Magistrate Judge's Act and Rule 41. Rule 41 itself does not appear to be a statute, but apparently -- well, I don't know. Does it have the effect of a statute?

MR. FIEMAN: It does, Your Honor. I have to find the exact provision. We did cite it. But Rule 41 was -- the statute is implementing Rule 41. So it's a very short statute. I will find the citation. So Rule 41 itself is statutory -- and I will give you that citation -- and therefore, we are dealing with two separate jurisdictional statutes, Rule 41 incorporated and then the Magistrate's Act. So they both have statutory effect -- and, Your Honor, I am sorry, I don't have that particular citation, but I do know where it is in the pleadings.

THE COURT: I don't know why our librarians don't do things the way I think they ought to do them, but having a rule and not having it cited as a statute, if it is a statute, doesn't make much sense to me. But that's besides the point.

I had another question, but now it escapes me.

MR. FIEMAN: The last thing I mentioned was the prejudice or the MAC address.

THE COURT: I know what I was going to ask. This new rule that would govern such matters, is that addressed to the

Congress or the rule making?

MR. FIEMAN: The way the process works is that DOJ, as we noted from the congressional research materials that we provided to you largely in response to the *In Re Search Warrant* case, the Texas case that denied the NIT warrant, then began requesting to the Federal Rules Committee -- I think the chair of that is Second Circuit Judge Raggi -- that there be a rule change, that it reviewed and submitted to the Supreme Court. The Supreme Court then forwarded its proposed change to Congress, and if Congress does not act on it, it automatically becomes a rule.

There are bipartisan bills pending in both the House and Senate to block that in large part because of some of the revelations in these cases. But you will also note, in terms of the congressional research report that we submitted to Your Honor, two things. One is that it is very clear that DOJ requested the rule change because they know the existing rules do not allow it. That's all in their analysis.

THE COURT: Okay. Go ahead.

MR. FIEMAN: There's a way to do this, and there will be new challenges and new issues depending on how that rule is drafted, the scope of the rule, but that's how the process works. You don't get ahead of Congress and decide: Well, we are going to interpret Rule 41 for our own purposes, despite the fact that Congress has codified in both the Magistrate's

Act and Rule 41 that we can't. So it was prejudicial, it was deliberate. And either one of these grounds alone would lead to suppression under Ninth Circuit law, Your Honor.

We've talked about the *Weiland* case at some length, its constitutional magnitude. If a rule violation like this is not of constitutional magnitude, I don't know what is. I mean, we are talking about core privacy interests. We are talking about jurisdictional interests. We are talking about the fundamental relationship between Congress and the Executive Branch when Congress makes laws and rules and the Executive Branch chooses to interpret them as they will. So there is a tremendous amount constitutionally at stake just folded within what seems like rule issues.

So let me turn to what the government ultimately relies on here, Your Honor, because I think where we stand is pretty clear; what happened is pretty clear. Ultimately, what they want the Court to find is good faith. Well, let's start with, again, Ninth Circuit law, the *Comprehensive Drug Testing* case, 621 F.3d 1162, and I have the relevant quotes from 1178 on the screen, Your Honor.

There, the Ninth Circuit, in another case where the government was, in their view, forum shopping and manipulating information between several different jurisdictions in order to obtain both search warrants and subpoenas, the Court there, just like in the *Sherman* case when it comes to distribution of

child pornography, the Ninth Circuit in this case warned the government about its approach to its representations to the courts that issued those search warrants and subpoenas, and they said that "omitting highly relevant information altogether -- and this is from either subpoena applications or search warrant applications -- "highly relevant information altogether is inconsistent with the government's duty of candor in presenting a warrant application."

And this is where -- you may remember, I think in the *Schesso* case, we struggled with CDT, Your Honor, and there was some forum shopping between state courts and federal courts going on there; you actually gave a suppression order there. But what we were focussing on there, and what's still highly relevant is again what the Ninth Circuit said, "a lack of candor" -- they are not even talking about *Franks* issues, they are talking about a higher principle related to the government's duty of oversight -- excuse me, the Court's duty to oversee the government -- "a lack of candor in any aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return evidence or suppress seized data."

So I have already listed a variety of ways that the government was less than candid. They are really hanging their hat on the fact that on page 29 of this application, there are two words saying activating computers "wherever

located." I am going to talk about how Judge Buchanan, I think, very clearly understood what they were asking for and how she dealt with it.

But to finish up with the argument, I would like Your Honor, please, to take a look at the warrant that the government submitted in the *texas.slayer* case, District of Colorado. This was a prior NIT case. It never -- I don't think they ever caught the target. It never was challenged in court. We also provided copies of the Nebraska warrants. They are saying, this is how they used to write their NIT warrants. Here, there they are asking for an NIT warrant for Colorado "and elsewhere."

They are forthrightly indicating on the cover, they actually amended the search warrant to provide this information that was going to be outside the district. They never went back to Magistrate Judge Buchanan here. So in Colorado and Nebraska and these prior NIT cases, they were never challenged in terms of the Rule 41 issues, so we didn't get rulings on that. But they put right on the face of the warrant, this is outside our district. Compare that to our warrant.

The only location specified in the warrant itself, or anywhere in the attachments, is Eastern District of Virginia, period. Why did they do that? Why did that change come? I will tell you why, Your Honor, because all you have to do is

look at the sequence of events. The Colorado and Nebraska warrants were prior to the *In Re Search Warrant* case by Judge Stevens in Texas, the very case that's discussed at length in the congressional analysis of why the DOJ is seeking the rule changes.

It's referenced, in fact, in the communications by the Department of Justice when they first sought the rule changes. What triggered Judge Stevens was that he saw that the warrant application was intended to be executed -- the warrant was intended to be executed outside his district. So what did they do? They stopped saying "and elsewhere."

Now, that's appropriate if you intend to be sincere about that, and Judge Buchanan, I believe, took that in good faith. You know, we keep coming back to what the government intended to do. They intended to catch pornographers, but the road to hell is paved with good intentions, Your Honor, and the reason we have rules is because when we have judicial oversight and we have the duty of candor, the courts need to weigh in, in a meaningful way, both before these types of warrants are issued and afterwards, which is where we are in this process.

So let's talk about what was presented to Judge Magistrate, Your Honor, and the claimed good faith --

THE COURT: Was there a record made by Judge Buchanan in her chambers when she issued this warrant? I assume she took the testimony of the person that signed the application.

MR. FIEMAN: What the government has indicated -- and not these two gentlemen, but what I have seen in other pleadings, so maybe they can clarify -- is that the paper application was simply submitted to the judge, and apparently there was no actual testimony or questions taken. So she relied solely on the face of the warrant for saying this was a Virginia warrant.

Now, let's talk about that warrant because this is a big part of -- and we think the simplest and indisputable way to suppression, Your Honor. Even if the government had been candid in the application when they stuck in -- on page 29 -- the very technical and dense warrant, that they were going to search anywhere, 120 countries, something that they already told Judge Raggi and the rules committee, they can't do. But let's put aside the fact that you can't reconcile that.

The face of the warrant controls. In the Ninth Circuit, you cannot reference the application to construe or interpret or expand the warrant, unless it's incorporated and attached. That's *SDI Future Health*, 568 F.3d 684. It's up on the screen, Your Honor, what they are holding. And Your Honor, why I say this is indisputable, it's because it hasn't been disputed. We cited all this Ninth Circuit authority in our brief.

We cited *SDI*. We quoted this text. It's another rule. In this case, it's not Rule 41, the Magistrate's Act or 3509.

It's the rule of construction that the Ninth Circuit has laid down. Well, I guess this doesn't apply to the government either.

So in the second quote I have up, Your Honor, the Ninth Circuit held as follows: The rules of construction for a warrant. "The warrant requirement is a means of preventing arbitrary and unreasonable invasions of privacy," and that's why all of this is of constitutional magnitude, but they held at the end, the search warrant itself, the actual warrant, "is the tangible evidence that precautions have been taken to ensure that no such invasion has occurred."

So what does the government argue in the face of this Hornbook, Black Letter Ninth Circuit law? They suggest it's Judge Buchanan's fault. They are saying that she signed a warrant that, even though judges are presumed to know and follow the law, that legal presumption, she knowingly signed a warrant -- that is, she can't sign under the Magistrate's Act -- they tell the Court that she knowingly signed a warrant that does not comply with Rule 41.

They say that she knowingly signed an unprecedented global warrant for 120 countries and the satellite that the Department of Justice in its own material says you can't issue; that she disregarded the fact that, as a core constitutional requirement, a warrant needs to be particularized as much as possible.

The government contends that Judge Buchanan got all that wrong or simply chose to ignore the rules so that they could pursue this investigation. She did that even though, according to them, she didn't amend the face of the warrant to say, for example, as they did in the Colorado warrant "and elsewhere," or "outside the state" or "internationally." She didn't bother to do that, according to the government. She did not stop to incorporate the affidavit by reference, by writing that in, which she would be required to do under all the circuits, and she also didn't bother to attach the affidavit.

So I guess all of this, Your Honor, is Judge Magistrate Buchanan's fault. I choose to believe that Judge Buchanan did something much simpler. I believe that she knew full well that her jurisdiction is her district; I believe that she approved a warrant that says on its face Eastern District of Virginia and did not incorporate or attach the application because she knows it was limited to her district, they could go after all activating computers there, consistent with the law and consistent with the rules.

Then they build their case, like they do in any other case, you keep expanding. You get maybe several hundred computers in Virginia. Those computers you search, people there who are distributing or downloading child pornography or emailing and sharing files, you get IP addresses off of their

email and file sharing for other districts, you go to those other districts, you get proper warrants, and then it takes a little more time and effort, but that's how you build a case.

The government, however, says no, what the magistrate did is she exceeded her authority under the Magistrate's Act and Rule 41 and issued a global warrant without even bothering to make her intentions clear or incorporate the application.

I believe that would be incompetent, and I don't believe that's true. I believe she did the right thing, she limited her warrant.

Now, Your Honor, I am near closing. I just want to say a little bit --

THE COURT: Don't say you are near closing unless you mean it.

MR. FIEMAN: I am much nearer. I just want to talk briefly about the probable cause issues because, Your Honor, one of the things you previously observed in a couple of my cases is that the broader the warrant, the more expansive, the clearer the facts in support of probable cause should be. It's just what the bedrock is.

Now, here we have a warrant of unprecedented scope, 100,000 computers, visitors around the world, a global warrant, based on what probable cause? Well, just going to the home page -- and we've submitted that the actual home page, not the one that was described in the warrant because

there's no child pornography on that home page, and people were -- the ITs were deployed as soon as they landed.

Now, in *Gourde* -- and I know this case, Your Honor, it was a very important case in some respects because the court was struggling -- the Ninth Circuit was struggling with, when do you get to search somebody's computer just because they are on the internet and maybe surfing or going to places in an exploratory way or whatever, or looking for kinky things that aren't necessarily illegal, when do you have enough to actually invade their home computer?

This is the *Gourde* case, and what they found -- there are certain principles that they lay out. First of all, they have to stress it was somebody who maybe got to that site and knew what they were getting into. Now, here they noted that the defendant had not taken advantage of any free tours and maybe after viewing, finding there was pornography, backed out of it. There was evidence that he had purchased a membership, had maintained it for several months and, most importantly, "he was not a person who became a member" -- I am quoting, this is on the screen -- "but the next morning suffered buyer's remorse" or a belated fear of prosecution and canceled his subscription.

People make mistakes, and they buy memberships to websites thinking that it's child erotica or all sorts of perverse things that you may find distasteful and illegal, but you

clearly have to show the person that you are searching, the target knew exactly what they were getting into. So compare *Gourde* to here.

Well, because of the government not letting Judge Magistrate Buchanan know that the home page had changed, that there was no longer any child pornography on it -- if you look at the home page, there's no reference to Lolita, no reference to child pornography, you are not required to pay memberships. There was -- they did not offer a free tour or a preview of the content, as was the case in *Gourde*. So a lot of these people -- and these numbers bear it out -- probably went there thinking they were getting into some kind of fetish site, an adult site, took a look at what was there maybe, backed out and never went back.

But this warrant, according to them on this probable cause, allowed them to search 100,000 people who just got to the home page, and they conceded that everything else in the home page, the technical language, that would not have meant anything to the casual observer, and in fact, it's commonplace for sites like Facebook.

So even though they are aware that what you see, the unabashed announcement, what they talk about in *Gourde* is the key to probable cause, when you are relying solely on accessing a website to do a search, they put an inaccurate description of that home page in the warrant. They kept that

home page the same the entire time; it wasn't that they even said, you know what, we see now that it was changed out, we need to put up the exact home page that we described to Judge Buchanan so that's consistent with the warrant. They didn't change it back; they had control of the site. They never informed Magistrate Buchanan that the appearance of the site had changed, even though, at least the Ninth Circuit, that unabashed announcement, that appearance, is critical.

Now, how do we know -- and then look at the scope. So Your Honor is concerned about both what facts were key for probable cause and then the scope. So the scope is, they claim authorization to search 100,000 computers anywhere in the world based on an ambiguous web page, with no particularized information about any of the targets that were going there, no collector profile, nothing to supplement it except what is on the home page. Well, out of that 100,000 visitors, they got 8700 IP addresses and they arrested now almost what, 18 months later, 16 months later, 214 people.

Now, I understand that's a little bit looking backwards, but I think it is really important. If this was so obviously a child pornography page, and there are 100,000 people going to it, well, then likely every one of them is committing a crime. And yet, even out of the 1152 investigations that the government says it has opened, according to its latest disclosure, they have made only 214 arrests, and as far as I

can tell, all those people are just for possession.

In the course of doing that, that classic -- it's a classic dragnet. In the course of doing that, they then pumped out a million or more images of child pornography. Let me just talk about how that works. Every time someone went to the site, and if they did want to look at images -- we don't know how many of these people actually looked at anything because there are all sorts of different sub-forums, but let's say they looked at them, they downloaded it, that's gone. That's worldwide. And a million images in the course of -- apparently 214 people out of 100,000 visitors merited actual arrest.

So, Your Honor, this is where we are at this point, and I submit this is our position. The government violated the Magistrate's Act. It's jurisdictional. It's dispositive. They knowingly and deliberately violated Rule 41, according to their own manuals that we submitted to you about the scope of Rule 41, that manual for prosecutors, the letters that they submitted to the rules committee, and all of the congressional analysis of why the rule change was proposed. They knowingly violated Rule 41. They searched unauthorized locations.

The face of the warrant -- which is all we can rely on, according to the Ninth Circuit rules -- says Eastern District of Virginia, period. They got a global warrant that is as close to a general warrant in the cyber age that we can really

envision, 120 countries worldwide, 100,000 people.

They were reckless at best about including a false description of the site. They told Magistrate Judge Buchanan that the home page contained child pornography. It did not. They utterly, utterly failed in their duty of candor. In the process of all this, when we are looking at the totality of the circumstances, they became, at least briefly, the world's largest distributor of child pornography and re-victimized countless children.

Your Honor, if all that does not require some measure of intervention and line drawing and deterrence by the courts in order to vindicate fundamental principles of the Fourth Amendment and due process in terms of the discovery issues and candor and respect for the rule of law, then we've seriously run the risk of the technology and the government unilaterally overtaking some very core values and very core rights.

So I close here as I started. There's something of a crossroads here, Your Honor, and obviously we hope you will take the right direction on this because a lot is at stake. Your Honor, I probably spoke more than you wanted me to, but I will end simply by asking if you have any questions.

THE COURT: One kind of side issue, I guess, is whether in your opinion the warrant is valid in the Eastern District of Virginia.

MR. FIEMAN: Absolutely, in terms of what it says on

the face of the warrant. Now, there are additional issues in terms of probable cause and all the other *Franks* issues, but in terms of the jurisdictional elements, yes, it is, and that's why several of those cases in the Eastern District that have come down really don't shed much light. But yes, I believe that's exactly what Judge Buchanan did, activating computers anywhere located within my district and then go build a case from there.

Anything else, Your Honor?

THE COURT: Well, I may have some more questions, but I will hold them for now.

MR. FIEMAN: Thank you, Judge.

THE COURT: It's a little ahead of the usual schedule, but I think it's appropriate to take a break probably before we hear from the government.

MR. FIEMAN: Your Honor, I just wanted to give you that citation, if I may, for the statute that makes Rule 41 statutory. It's 28 U.S.C. 636. So both the Magistrate's Act and Rule 16 are statutory.

MR. GOLDSMITH: Your Honor, before we take a break, I would like to make just a few short comments on behalf of Mr. Lesan.

THE COURT: Thank you.

MR. GOLDSMITH: I will make an effort not to repeat anything Mr. Fieman said. I just have a few comments about

the motion to exclude on the discovery issue related to what the government's expert testified to yesterday. He used two analogies, Your Honor, that I think we can use to support our position. One is that he argued that in a burglary case, you would be concerned with two things: How the burglar got into the house, and what happened after the burglar was there.

The exploit is -- to analogize -- is how the burglar got into the house. And in any burglary case, someone would have to prove both of those things, how the burglar got in and then what happened afterwards. We are being deprived of the evidence regarding how the burglar got in, so to speak.

Going further, their expert analogized the exploit to a key, something that sounds very simple, but he didn't examine the exploit. He agreed he did not see it, he does not know what that code is. And he's coming up with an argumentative analogy: What if that exploit isn't a key, but it's a battering ram? What if it's something that blows the door off of the computer? We don't know that. And that's why it's relevant to the defense, particularly in the search context. So I want the Court to think about that as well.

In terms of the search issues themselves, just last week on October 26th, the government sent us some discovery. And interestingly, there were a couple of memos where the FBI was explaining what this investigation was, and I am going to read just the beginning sentence from that -- those two memos, and

it's the same in each memo.

It says: "Operation Pacifier is an international investigation into a Tor hidden service known as Playpen and its users." The key word there, Your Honor, is "international." Nowhere in any of the warrant documents, the application, the warrant face itself, do they use that word "international." How is a magistrate judge to know, when they know their investigation is international and they never once use that word, the only word that we've heard already is buried on page 29, paragraph 45, that the computers wherever located. That's it. We know under Ninth Circuit law, that particular line cannot expand the warrant. That line cannot expand the warrant. Ninth Circuit law is very strict on interpreting warrants. It was not a magistrate error.

Secondly, some of the additional information they gave -- and I think the Court heard these numbers. There were approximately 8,713 IP addresses derived during this investigation. That's something we learned just late last week. Of those 8,713, 7,281 of them were foreign. So the vast majority, something like 84 percent of the actual materials they got through the NIT, were not on U.S. soil. This was really a truly international warrant, and they never used that word.

Your Honor, it is very clear to me that the government was not engaging in their duty of candor with that magistrate.

Those are the points I wish to make.

Thank you.

THE COURT: Thank you.

MR. HAMOUDI: Thank you. On behalf of Mr. Lorente, we join every argument made by defense counsel. We'd like to highlight on the issue of the warrant. Just to let the Court know, Congress granted the Supreme Court authority to write Rule 41 under the Rules Enabling Act. That's Title 28, Sections 2071 to 2077. And then the Supreme Court submitted its proposed changes to the rule this past April 28, 2016, under Title 28, Section 331, to Congress for approval.

But the proposed change for the rule was made in September 2013, and the reason that it was made was for two common investigative situations. One was when the warrant sufficiently describes the device to be searched but law enforcement do not know the location of the target's device. That raised particularity problems.

The second was, where the investigation requires officials to engage in surveillance of numerous computers in multiple jurisdictions, and that's the issue with the Magistrate's Act and the general warrants argument that we've been making.

What does that tell us? It tells us that they have known the problem with these types of investigations since September 2013. And if they know that, then they are going to Magistrate Judge Buchanan in around 2014 and they are trying

to get the search warrant, and they know that there's problems with the rules, and yet they go ahead and conduct a search that is now revealed to us to be an international search. That's our issue.

At the end of the day, we believe that there is a difference in opinion as to how one views the Fourth Amendment. The government views the Fourth Amendment as a road map on how to search and seize. We view the Fourth Amendment as a restraint, as a protection of privacy against unreasonable searches and seizures, and we are asking the Court to embrace the latter view, not the former view.

On the issue of materiality, we are not required to disclose what our defense is at trial. We don't have to, because all we can do is sit quietly and make the government carry their burden of proof. But what that witness yesterday said, he said on the stand, you don't need to look at the code because it is redundant. He is getting contract grants from the FBI.

With all due respect, we have an obligation to attack that line of testimony with our own experts with an opportunity to view the evidence through our own expert's eyes and let a jury decide whether or not it is redundant. We don't think that he gets to decide that question.

We don't believe that these issues need to be resolved behind closed doors. We think 12 jurors need to sit and

decide whether or not we can impeach the whole government's investigation of this case, not to trust any evidence that they present in this courtroom because of what occurred here. We have that right. That's it, Your Honor. Thank you.

THE COURT: Thank you, Mr. Hamoudi.

We'll taken 10 minutes.

(Morning recess.)

THE CLERK: All rise. Court is again in session.

THE COURT: Please be seated.

MR. HAMPTON: Your Honor, Mr. Becker and I are going to divide the presentation here, so I will address suppression.

THE COURT: Just a second, I've got to get this.

MR. HAMPTON: So I will be addressing the suppression and very, very briefly, the outrageous government conduct, and Mr. Becker will be handling the discovery issue and the exclusion motion.

THE COURT: All right.

MR. HAMPTON: Your Honor, I think an important preliminary point is a theme that has emerged, and a theme that I think the defense has pressed, is essentially the government did a lot of bad things and all that adds up to some kind of sanction, suppression, dismissal, whatever it may be. I think it's important to remember, that's not the analytical framework that this Court has to look at this.

If the government did things that it's not permitted to do, there are certain legal frameworks, certainly there are remedies for those legal violations, but the two have to be tied together.

In the context of outrageous government conduct, when I said that reasonable minds could differ, I did not mean to suggest that reasonable minds can differ about the need to follow the law. Reasonable minds can differ about the costs and the benefits of a particular operation. Reasonable minds can differ about when balancing those costs and benefits, what is the best way for the government to fulfill its mission to stop horrific child sexual abuse and investigate crimes that, even as defense counsel described yesterday, even assuming the defendants here are simply mere viewers, cause profound societal harm, and what is the best way for the government to conduct those investigations when the defendants are operating in the dark, anonymously and with impunity.

We can all talk about whether a given operation can be done differently or better, but the question is did the government act outrageously, did it act unfairly, did it violate the due process clause in such a grossly offensive way that the Court's conscience should be shocked.

Indeed, did the government act so heinously that it's appropriate to allow criminals who have committed serious, dangerous, violent offenses to go free. Because that is the

position that the defense has taken, and that is an outcome the government can't live with. So I would urge the Court not to go down that path and deny that motion.

I will just flag one issue just as to 3509, that is -- and I believe defense counsel cited it as 3503 -- I think it's 3509. It begins with the language "in any criminal proceeding." It is a statute related to criminal discovery. Again, as I said, this Court, other courts, other people may disagree about the government's chosen investigative technique, whether those benefits outweigh its costs, but it was what the government thought was appropriate to deal with a very challenging problem.

That turns me to suppression and the defense's Rule 41 arguments. I will note that the defense spoke a lot about the Magistrate Judge's Act, and the fact is their argument collapses into one. If there are Rule 41 violations, they say the Magistrate Judge's Act was violated. If there were no Rule 41 violations, the Magistrate Judge's Act was not violated, because after all Rule 41 would have permitted the Magistrate Judge to issue that warrant.

So the commentary there isn't really all that important. The implications of what the rule means, I am going to talk about that, but the issue is, did it violate Rule 41? Before that, though, before I go into the details of the suppression argument, I also want to address the discussion of the

government's lack of candor.

The notion that Magistrate Judge Buchanan could have read that 29, 30-page affidavit, and that search warrant and not understood exactly what the government intended to do is preposterous. The warrant face sheet by itself, which we can pull up --

THE COURT: I have got the warrant here in front of me, if that's what you are going to refer to.

MR. HAMPTON: So if you go to Attachment A, the government's intent and the authorization it sought is clear: "The warrant authorizes the use of a network investigative technique (NIT) to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below." And then it describes exactly those two terms.

A computer server. It is a server operating on the Tor child pornography network website, referred to herein as the Target Website, identified by a specific URL, and located at a government facility in the Eastern District of Virginia. The activating computers are those of any user or administrator who logs into the Target Website by entering a username and password.

The internet is a global network. It is playing from that face sheet, that attachment that the government had control of a website accessible worldwide, and that it would deploy a NIT

-- and that it's established that website in the Eastern District of Virginia where that warrant was sought, and that it would deploy a NIT to any computer whose user entered a username and a password, who had entered the Eastern District of Virginia and entered that website, they would be a target of the NIT.

It's simply strange credulity to think that Magistrate Judge Buchanan could not have understood exactly what the government was doing. And the notion that the government was not being candid or was somehow trying to hide the ball presumes, of course, that the government had accepted that this was not an appropriate theory, that this was not something that the government can do.

But of course, the government has maintained throughout that Rule 41(b)(4) -- among other provisions -- but 41(b)(4), the tracking provision, is sufficiently analogous to this situation to embrace these types of warrants. That is an argument that this Court did ultimately reject in *Michaud*, although noted that it didn't strain credulity, that it had some merit at least, but it is a position that at least seven other courts within the Eastern District of Virginia and elsewhere have embraced.

That the government can be accused of bad faith or of not being candid with a magistrate judge simply because it did not agree with the narrow and very craft interpretation that the

defense now wants to force upon it, is not fair and is not an appropriate inference to draw.

As for the international flair, the international impact of this investigation, it is true that the internet is a global phenomenon. Computers from all over the world could have accessed -- and as it turns out, did access this website. I will note that the report referenced by Mr. Goldsmith was written after the investigation -- after the IP addresses had come back and the government had been able to identify where those IP addresses were.

But even the affidavit that was presented to Magistrate Judge Buchanan noted that there were foreign language forums on the Playpen website. So it was certainly possible, but the fact is the three defendants here were not in another country; they were in Western Washington.

It is not their role to assert whatever protections those in another country might have, although I would note that those individuals reached into the United States to trade and to access child pornography. So regardless of what the law may ultimately say about someone who is prosecuted in another country, that's of no concern to the defense, and it's certainly no justification for suppression here.

So that brings me to the challenges that are at issue here. The government filed a detailed affidavit from a veteran FBI officer explaining why this Tor website Playpen

was hard to find. It was not something that someone would simply stumble upon. It explained that its home page had images of young girls that conceivably changed just before the warrant was signed, but it wasn't changed to remove those images of young girls in a sexual pose, it's just that there was an image of one young girl in a sexual pose.

The affidavit talked about all of the things that he knew, based on his training and experience, were suggestive of a child pornography website, the focus on privacy and avoiding detection. And then, of course, he detailed the content of the website which was devoted to the discussion of and the trafficking in child pornography.

There was ample probable cause to support a warrant to search -- or to deploy NIT to any user who logged into that website. There was absolutely a fair probability that anyone who had gone through the steps to find that website, create an account and log in, was there for the purpose of the website, to trade child pornography.

Defendants posit a contrary view and they, of course, note that there's another case, another website case, *Gourde*, where probable cause was found. And in their view, because probable cause was found there, it can't be found here. And it's true, there are different websites, but the same factors that supported the finding in *Gourde* don't necessarily have to be found here.

There are different facts and circumstances, facts and circumstances that haven't been explained away. And the fact that the defendant may disagree with an experienced FBI agent's assessment of the meaning of this information isn't relevant to the probable cause inquiry. Nor are the defendant's claims about information regarding IP addresses and what was collected as a result of these NIT deployments, the number of investigation, number of charges.

When a search warrant is authorized to go into someone's home to look for drugs, if there's probable cause to search for drugs, there's probable cause whether or not the drugs were actually found. We don't look at what happened after to evaluate whether a search warrant exists, a search warrant was valid. That's not how the inquiry works.

Now, as to Rule 41, the government has explained why it believes that this warrant was appropriate under Rule 41, a rule that is intended to be interpreted flexibly, to allow the government to investigate crimes but also comply with the Fourth Amendment. Plainly, there's a disagreement among the courts, there's no question.

Seven courts have concluded that the government's theory of this warrant as an appropriate tracking warrant is valid. Many others have not, including this Court; however, those same courts have concluded that is not a violation that's appropriate for suppression. So the ultimate question here

is, wherever the Court may come out again on the Rule 41 violation -- and we would urge the Court to reconsider how it evaluated that question in light of the other decisions that have been handed down that we've noted in the appendix -- the question is, if there were a Rule 41 violation, is suppression appropriate?

The defense's argument can be summed up as, of course suppression is appropriate because Rule 41 was violated. That is their theory of prejudice, that is their theory that the warrant was void ab initio. That is their theory of deliberate error. It all comes back to well, the government violated Rule 41 and we're done.

The government approached a neutral magistrate judge with a detailed affidavit establishing probable cause and identified particular locations to be searched and particular evidence to be seized. That is what the Ninth Circuit has noted as a fundamental policy of the Fourth Amendment. So if the Court believes there's a violation and believes that suppression is even a possible remedy, what the Court must look to is what are the interests in suppressing evidence, what are the benefits to suppression and the costs, and how do they balance that.

The Supreme Court has made absolutely clear that suppression is a last resort. It is not a first impulse. That is true --

THE COURT: Mr. Hampton, before you talk further about suppression or not suppression, let me ask you about Rule 41.

MR. HAMPTON: Of course.

THE COURT: What is the government's position on what portion of that rule gave authority for this particular warrant? Is it the tracking device portion or some other portion of that rule?

MR. HAMPTON: Your Honor, I believe in our briefing we identified two portions, and I think, though, that certainly the stronger argument and the argument that I think is the most logical fit is the tracking device, which is (b)(4).

THE COURT: Now, what was the tracking device here?

MR. HAMPTON: The NIT, which was deployed in the Eastern District of Virginia.

THE COURT: All right. Did the NIT have on it the exact date and time that it was installed and the period during which it was used, which is required also by Rule 41 on a tracking device?

MR. HAMPTON: I apologize, Your Honor, that I don't know the precise technology and know whether it had those particular things -- yes, Your Honor, there was an exact date and time when the NIT would have been deployed because at the time the NIT was deployed, there was a log-in that prompted

that.

THE COURT: Where is that?

MR. HAMPTON: Pardon?

THE COURT: Where is this record of deploying a tracking device?

MR. HAMPTON: It would be at least in the signature report and probably other server records, but the signature report which is the report that details a given user's activity on Playpen.

THE COURT: A tracking device is defined in 18 U.S.C. Section 3117 as "an electronic or mechanical device which permits the tracking of the movement of a person or object." We are not talking here about persons, but what object?

MR. HAMPTON: Well, the code that would have been distributed when someone logged into the Playpen site, so that content -- the NIT accompanied that content as it was deployed on the server.

THE COURT: You see, here is what I am headed to or what's of concern. A tracking device is not designed under Section 3117 to track other than a person or object. But in Rule 41, you are talking about information as property, and it was used apparently here to track information.

You know, the language of the statutes and the rule seem to indicate that a tracking device is something very different than a computer NIT or some electronic communication between

computers. I know other judges have decided that was a good niche to hang their opinion on there, but I have a little trouble with that. It seems to me it's stretching the tracking device rule and statute beyond its intended meaning.

Do you have any comment on that? Now is the time to make it.

MR. HAMPTON: I understand why the Court is struggling with that, and I think it's accurate to say that the rules and the statute may not have entirely caught up with technology. However, the Supreme Court, other courts have directed that Rule 41 itself is to be interpreted flexibly. It is to be interpreted in a way that preferences warrants, that preferences exactly what law enforcement did here, which was identify a difficult problem, come up with a creative technological solution, and then seek an appropriate warrant --

THE COURT: What limits the flexibility of Rule 41? How far can you go?

MR. HAMPTON: Your Honor, I think it's tough to set what a particular outer boundary is. Unfortunately, that has to be done in an individual case. The government maintains that this Rule 41 is sufficiently flexible to accommodate this particular type of technology, something that tracks software code, that starts in a known location and then, as a result of the defendants' -- or the own conduct, travels somewhere else.

THE COURT: Okay.

MR. HAMPTON: In the end, if the Court remains unpersuaded that Rule 41 can accommodate this type of technology or this type of investigative approach, the question is should this evidence be suppressed? I apologize, I started with a balancing, but I think the beginning point is, does the good faith exception apply?

So even if there were some Rule 41 violation, was the government's reliance on this warrant reasonable such that it's not appropriate to suppress? And the government's reliance was reasonable. The fact is, courts are struggling with this very definition. There is difference of opinion among the federal courts. It is hard to understand how the agent who sought this warrant and the executing officers could be expected to have firmly resolved something that even the courts are struggling to figure out.

It's no answer to say the Department of Justice has advocated further clarification to the rules. The fact that the government and law enforcement agencies recognize that technology and the letter of the rule have not married up as yet is not evidence of bad faith or unreasonableness for the government to do what it believes the law permits, but also advocate for clarity.

As I said, the Supreme Court has made abundantly clear that suppression is not where we start, but it is where we

end. That is true in the constitutional context, and it would make no sense for there to be a different approach to a violation of the rules. The Court, to suppress here, must examine the benefits of suppression, that is deterrence of government misconduct, and balance that against the tremendous social cost of suppression.

THE COURT: Arguably, to do that you are throwing out Rule 41 and the Magistrate's Act and going right back to the Constitution and saying well, this is a reasonable search, under the Constitution.

MR. HAMPTON: I am sorry, Your Honor. There is a beeping sound.

Well, Your Honor, I think it's not so much throwing it out as we are in a situation where there is a warrant that has been issued and a finding of a rule violation on what I think can only be described as a close call at best. I mean, certainly the government thinks there was no violation, but even if there were, it's a close call, and so we have to decide whether suppression is the appropriate remedy here.

It wouldn't make a lot of sense if, in other contexts where there has been suppression, where a warrant fails some constitutional defect, it wouldn't make sense for suppression to be automatic there when here, there was a warrant supported by probable cause presented to a neutral and detached magistrate judge that identified with particularity the things

to be seized and the locations to be searched.

To be sure, it was potentially a large number of locations, and that's something that the defense has raised a lot of concern about, but there's no upward boundary. And if there were, how would it be chosen? A thousand, five thousand, ten? That's not really a meaningful discussion. The question is: Was there probable cause or was there not? And there was.

The costs of suppression here are tremendous. Defendants who committed horrific crimes could well be let go and go free, and the interest that would vindicate is at most a venue revision. It certainly wouldn't deter government misconduct. What government misconduct was there? The government did what the Fourth Amendment -- what is a fundamental policy of the Fourth Amendment.

It sought a search warrant from a magistrate judge, a magistrate judge in the district that it believed had the most logical and most appropriate connection to the crimes being investigated and the particular investigative technique. If the government in hindsight got that wrong, how will suppression deter it from getting that wrong again?

It is a close call. It is a complicated issue. And the answer can't be that the government just stops investigating certain crimes because there are questions and it has to make difficult calls about how to go forward. On balance here, the

government did what was necessary to protect these defendants' privacy interests because it sought a warrant.

And even if the Court believes the government should have sought a warrant somewhere else or that this particular district was not authorized to issue that warrant, suppression is certainly not going to further any constitutional interest and will further no deterrence interest.

I would urge the Court to deny the defendant's motion to suppress.

THE COURT: Thank you, Mr. Hampton.

MR. BECKER: Thank you, Your Honor. Good morning. I will move to the issue of the defense motion to exclude. I am also happy to address any questions the Court has on any of the matters that are raised.

Your Honor, you started out yesterday with a premise, and that premise was that you believe that the notion is that these cases are in fact separate from the *Michaud* case and need to be taken up on their own merits. We think that's appropriate and certainly a correct view of the Court. So I want to start with just some key differences between this case and this record and the *Michaud* case.

For one, there's been more information that was disclosed to the defendants in these cases. In particular, they have gotten the software that generated unique identifiers related to the NIT and can analyze that. We are also proceeding now

under the Classified Information Procedures Act. That is significant. It means that the public's interest in nondisclosure the government has not provided is heightened, and that does need to factor into the sort of balancing that Your Honor is ultimately going to undertake between public interests and the defendants' particular interests in these cases.

Your Honor has heard testimony from Professor Brian Levine, the only testimony that Your Honor has actually had in these cases, the only person who is an expert who you've had the opportunity to hear from, to assess credibility, and who's been cross-examined.

Professor Levine's testimony certainly, we submit, Your Honor, makes it eminently clear that the additional information, the narrow band now of additional information that the defendant seeks, would not actually further or be helpful in terms of evaluating or bringing their defenses, and I will talk about that in more detail.

All of these defendants, Your Honor -- and here's a critical point that I really want to engage with the Court about -- all of these three defendants are charged only based on information that was ultimately found on their computers after their home was searched. None of these defendants are charged with accessing Playpen. None of these defendants are charged with receiving child pornography from Playpen. That

is a critical difference, and it's a critical point for this Court.

It's so critical because it means that the NIT is not evidence in this case. The NIT will not be a part of the government's case-in-chief. The NIT is not necessary, nor will it be used to prove whether any of these three defendants were guilty of possessing or receiving child pornography that was found on their computers.

That's critical because that makes this case different than *Budziak*. In *Budziak*, which the defense has talked about, the technology that was used, the peer-to-peer technology that the government used, was central to the government's case against the defendants. It was the only way the government could prove that those defendants had distributed child pornography. That is vastly different than this case. We are not using the NIT as trial evidence. So we have to analyze the defense request for the information and their ability to mount the defense under that light and from that perspective.

Finally, Your Honor, all of these defendants have either confessed to or made statements to others about their personal involvement with child pornography. That is a distinguishing factor from the factual scenario in *Michaud*. We are dealing with individuals who made admissions to their child pornography-related activity.

So with that said, Your Honor, CIPA provides a framework

for this Court to analyze the issue between the narrow band of information that has not been provided to the defense, and I say that, Your Honor, because I think the defense has tried to make so much more of how much information that is, than is really accurate.

The NIT conducted a search of a defendant's computer, and that search provided particular information to the government, an IP address, a MAC address, and a little bit more information about that computer. All of that information has been provided to the defense. The computer instructions that conducted that search have been provided to the defense. A data stream, packet capture that shows that data going from the defendant's computer to the government's computer has been given to the defense. That's the NIT search. They have it all.

They have all the ingredients necessary for their six or 600 experts that they want to employ to do the sort of examination and analysis they want to do, to learn about the government's investigative technique. So it's in that light, Your Honor -- beyond that, they have the unique identifier generation code, they can analyze it, they can determine as we have that it works exactly as planned and as advertised.

The only piece that the government has not provided is the exploit piece. It is the means of access into a computer. That term, that understanding, Your Honor, is critical. What

we are talking about here is the means of access to get the code we have given them that ran the search onto their computers, and that's all. That's all we are talking about.

So there's a three-step process that CIPA mandates. One, is that information relevant and helpful? Two, is the information properly classified? Your Honor has already made rulings related to that. And the third part is a balancing of the sort of the interests that exist between the nondisclosure of that information and the necessity of it in light of all these factors.

Under CIPA, there's an important factor, an important piece or way that the Court can accommodate these interests, and that is the option of allowing for a substitution of information or a stipulation, rather than the classified information at issue. That's ultimately how we believe Your Honor should resolve these sorts of issues, rather than taking the extraordinary remedy of essentially suppressing all of the government's evidence against all these defendants.

Your Honor, first, we believe that the record supports our argument that the exploit-related evidence is not in fact -- and would not be relevant and helpful, either for the defense to mount a defense or to evaluate it. Now, if we limit ourselves to talking in generalities about how the defense wants to know how did the government technology work, what did the government do in general terms, and how did they do it,

it's not going to get us very far because they can always come up with some reason of curiosity as to why they think they are entitled to review information.

Curiosity is not the same as materiality. Materiality has to be tied to some particular defense. And when you look at this more concretely, when you dig into what's the information they don't have and what would they actually be able to do if they got it, you can see that it's neither relevant nor helpful, and here's why.

Knowing the method of access of someone into a computer does not tell you what happened after it was accessed. Here, what happened after the government accessed the defendant's computers, was that it ran the NIT code, the payload, the information that we have given them, and it collected the information that was authorized and we've given them that information as well.

Knowing the method of access does not tell you what happened once you were on there, just as knowing whether someone who ultimately took information from a home went in through a door or a window doesn't tell you what they did once they were inside.

Again, we've got to look at it even more carefully, Judge, because there's a couple of options here in terms of what would you ultimately -- what would you ultimately understand by reviewing the method of access, right. So one is, you

might understand that the method of access did not make any permanent changes to the user's security settings, right, that the method of access didn't break a lock or break a window.

If that's what you find out, then okay. That means, one, it's possible that somebody who knew that method of access, other than the government, could still have used that same method of access and done something inside their house, right? So that's one option. You review the method of access and figure out oh, okay, it's a window, and what does that tell you? Not very much, because as of right now it is possible that someone who knew the same method of access could also have used that method of access to do something inside the house, to run code on someone's computer. That is a possibility right now, that would remain a possibility after any analysis, so that gets you nowhere.

Option two, you review the method of access and determine okay, this did in fact or could have made some changes to a user's computer setting. All right, it turns out this way of getting in could damage a lock or it could damage a window. Okay, so you still have to look inside the house and figure out -- so now you know all right, it's possible that someone who knew this method could have gotten in and damaged something. You might also know okay, the government damaged something when they got in.

That means that someone with knowledge of this way of

getting in, or someone who came in later, could have done something inside the house. Either way, you have to determine what happened within the house, no matter how someone entered, no matter what the method of entry was, the possibilities remain that somebody could have gotten in that way or some other way.

Knowing what the method is or even whether the method made some changes or didn't, just doesn't tell you whether or not somebody else got in and made changes, whether somebody else got in and took something out, whether somebody else got in and planted something there. That's why this whole realm of discovery is not material, and it's not helpful because the possibilities will always remain.

It will always be possible that somebody knew of the same exploit. It will always be possible that somebody could have gone in and delivered malware through any means of vulnerabilities. That's just a reality of computing and the internet and malware. The defense's answer to this concept is to say well, our experts can't reverse engineer what happened. Well, Judge, that's -- it's a curiosity interest. It's not an interest that's tied to some particular defense.

They can evaluate whether or not they want to raise a malware defense based on their experts, based on their examination of their computers. Look at the computers and determine, is there malware on here? What are the security

settings? What would those security settings on the computer tell your experts could possibly have been done on a computer, and then argue and evaluate your defense from that.

You'd have to go through all of those steps whether or not you knew or ever looked at the method of access, because it doesn't matter. The key is what's on the computers, what's the evidence, how did it get there, what can you show from the settings of that computer to be able to evaluate or assert we think somebody else put it here, or we think it could be the case that somebody else put it here, or the government can't prove that I put it here.

All of those things can be done by looking at the computers, looking at the settings, evaluating that information, and you'd have to do that regardless of whatever the government's method of access to get the NIT code there was.

So there's still a balancing for the Court to strike here, Your Honor, and we have a proposal about how the Court can do that without having to go the extreme route of suppressing all or excluding all of the government's evidence, and that's -- one of the things the Court can do is substitute a stipulation or make a substitution.

So here's our proposal that we think would adequately allow the defense to put forth whatever defenses that they want to ultimately go forward with. The government used an

exploit to deliver a NIT to the defendants' computers. The government has not disclosed that exploit to defense for review. It is possible that an exploit can make temporary or permanent changes to the security settings of a user's computer which could allow someone to run commands on that computer without the user's knowledge. We will agree to that. We will stipulate to that. And here's the -- that gives ultimately the defendants their best case or whatever case they wish to make.

We are unable to counter the assertions the defense would make about the possibility of alterations to security settings, about the possibilities that the exploit could have opened some hole that somebody else used to run commands. We can't counter it because the exploit is not available to us to use as evidence. We'd be stuck with that stipulation and those possibilities, and the defense can use that to mount whatever defense they want. We have no trump card. We can't put the exploit into evidence because of its status.

In this scenario, if that's the relief the Court would grant, as we ask Your Honor to do, we won't do. The Court can order -- the Court can prohibit and exclude that evidence. The Court can prohibit us from putting that on. I tell you that we wouldn't be able to again because of its status anyway. So the defense is free to run whatever exams they want on their computers, find whatever malware or information

or evidence they can and put forth those defenses.

So ultimately, Judge, we think that in view of the drastic nature of effectively a sanction or the excluding of all of the evidence that's tied into this case, this is a better solution that strikes a better and appropriate balance among all the interests here.

There's huge social costs to this community of the Court excluding effectively all the government's evidence against three individuals who are charged with some serious crimes. We've heard over and over the crimes that they are charged with, minimized by the defense in asserting that these are individuals who are somehow low-level offenders who don't pose any danger to that community -- to this community. It's just categorically wrong, Your Honor. I am sorry, but we are dealing with Mr. Tippens --

THE COURT: You know, you talk about huge social costs. There's huge social costs in constitutional violations too, if this amounts to that. So you know, you can't ignore the Constitution in order to arrest somebody because they need to be arrested. So that's a balance. It's a balance beyond the details of what we are talking about here.

MR. BECKER: We certainly agree, Your Honor. That is absolutely the sort of balancing Your Honor has to undertake. My point is that the defense continues to minimize, frankly, the importance, the significance of these defendants because

of the charges they face, that they are only watchers or however they want to call it. That doesn't capture the interests that are at stake for this community and that need to be balanced.

We deal with that as part of the facts here. So when law enforcement goes into Mr. Tippens's home at the time they search his home, he has on a loop playing on a big screen television in his home video of a toddler-aged child being raped. That's a community concern. That's not someone who is not a series offender, who is not worthy of prosecution, who is someone that this community shouldn't be concerned about.

When law enforcement goes into Mr. Lesan's home, they find cameras in the bathroom of the home designed to catch occupants, including children, in intimate situations.

When law enforcement searches Mr. Lorente's home, they find a blowup doll with a child's face taped to it within that home, and there's evidence that he was filming other young children in his neighborhood.

So -- and I say that -- these are allegations. Ultimately, these are issues for trial, but we can't lose sight of the fact that these are not offenses that involve just pictures. These are offenses that involve individuals and defendants who pose -- in a community, our community, this community -- who pose a danger. That's an interest that this Court obviously is and should be concerned about.

So with that, Your Honor, we certainly understand there are tremendous interests that need to be balanced here. That is -- we understand it's a challenging job for Your Honor and for the Court. We believe that the appropriate balance to be struck here on both of these ends, on the issues of the suppression for the warrant as well as the issue of whether to exclude evidence, should not be struck by throwing out all -- effectively all of the government's evidence in these cases. We think that something less than that would accommodate the privacy interests, the ability to ultimately raise defenses.

I am happy to address any questions that Your Honor has.

THE COURT: Thank you, Mr. Becker.

Finish yours in 10 minutes.

MR. FIEMAN: Easy. Let me go through this quickly. One, in regard to the tracking device, if that's what they are hanging their hat on, that's fine. Two things: Mr. Becker himself told the Court -- and I just wrote this down -- the NIT conducted searches of defendants' computers. The computers are in Washington. The tracking device has to be installed within the district in which it is authorized. This is not tracking. This is seizing. It didn't just track information, it actually captured MAC addresses, IP addresses, and all sorts of data from the computers. So it was a search, and it was not within the district. The tracking provision does not apply.

Now, you asked, Your Honor, a very interesting question. You asked where the installation records for the tracking devices are. Well, where they are saved, Your Honor, is on the server component. That is one of the components we've been asking to look at from the beginning because that's essential to the chain of evidence, chain of custody, and that goes to a very important Fourth Amendment issue, exactly when and how and where this was installed. All that data is in the server component. The government will not disclose it.

In regard to probable cause, Mr. Hampton was talking a lot about content. The reason that the *Gourde* case, and all the other cases that, Your Honor, cited in the government's memo, if you look at Document 74, our suppression motion at 21 to 22, we talk about cases like *Martin*, *Fasso*. Those are all from the government's pleadings.

All those cases said is you cannot base probable cause on merely accessing an illegal website, all of it. Every one of them said that you have to show that there was ongoing membership and opportunity to view the content or other indications that somebody didn't just look at the site and walk away.

All of these NITs were deployed at the home page. In the *Fasso* case, cited by the government, in fact said there was no probable cause when the application failed to allege that the defendant had not only entered the site, but likely

downloaded.

Your Honor, in regard to 3509(m), that provision in terms of custody and control of child pornography provides explicitly in any criminal proceeding, and it includes investigations, and then a subdivision relates to discovery.

Now, in terms of the good faith exception, Your Honor, we cited case law that clearly states that you cannot even invoke the good faith exception when the government itself is responsible for the errors that the magistrate relied upon. You only get to invoke good faith if the warrant is issued and it's a reasonable warrant and the government relied on it, but when they are responsible for omissions or errors in terms of the application, they cannot even invoke it.

Now let's talk about the exclusion issues, Your Honor. Mr. Becker proposed a stipulation to resolve this. Well, *Soto-Zuniga* talks not just about at the time of the trial, it talks about pretrial motions, Fourth Amendment issues, suppression issues. So let me propose this. If the government is prepared to stipulate that the NIT exceeded the scope of the warrant by seizing unauthorized data from the clients' computers, we will entertain that stipulation. But unless we get that, we will never know.

Let me talk about the exploit very briefly. It is not a key. Please go back to Professor Levine's testimony. I asked him -- I put up Professor Miller's declaration. The exploit

doesn't just unlock a door, it can change settings, it can alter data, it can take down the security settings permanently. So I challenged him specifically on that. It is not a key. It is simply -- when you are breaking in, you may also leave the door open, you may damage the furniture, you may plant evidence behind. All those things happen from the exploit. So I don't want to get caught in the semantics, but the government trying to carve it out in that way is just not consistent with any of the experts, including their own.

Now, Your Honor, Mr. Becker finally spent a fair amount of time talking about additional evidence that shows -- evidence unrelated to the NIT that may show possession, statements from the clients. Well, two things about that. First of all, we submit all that evidence is fruit of the NIT search and, to the extent that the government shows that it's not, they are entitled to proceed on that untainted evidence.

Finally, Your Honor, if we exclude all fruits of the NIT and simply what's left is evidence that is untainted, we can go to trial on that. There might be a possession count. They simply cannot prove receipt without any data disclosed to us in terms of how those particular images ended up on the computer. For all we know, it was a third party attack.

So with the proposed stipulation that I have made, and with excising all the fruits of the NIT evidence, if the government has evidence left over that they are prepared to

show established possession then yes, we can go to trial on that, Your Honor.

Thank you.

THE COURT: Any other comments?

MR. HAMOUDI: Nothing else, Your Honor. Thank you.

THE COURT: Well, there is a lot of information here. Courts all over the country are going all sorts of different directions. We'll have to write on this, and there are many decisions I have to make along the way to get to conclusions.

We'll work on it and try and get it to you quickly. I have got trials backed up here now so I am not sure just when we'll have the kind of time we need to finish this, but we don't sit on things for long.

Okay. Well, I don't think I have any other questions. You've given me all the information that a guy can want in these situations. You know, I have been at this for -- gosh, I think it comes out to about 48 years now, and there's some cases that come along that make you feel inadequate, and this is one of them. So we'll do the best we can with it.

MR. FIEMAN: Thank you, Your Honor.

MR. HAMOUDI: Thank you, Your Honor.

MR. BECKER: Thank you, Your Honor.

(Proceedings concluded at 11:56 a.m.)

* * * * *

C E R T I F I C A T E

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/S/ Teri Hendrix **November 21, 2016**

Teri Hendrix, Court Reporter **Date**