IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Newport News Division

UNITED STATES OF AMERICA, Plaintiff, v. EDWARD JOSEPH MATISH, III, Defendant.	CRIMINAL CASE NO. 4:16cr00016

TRANSCRIPT OF PROCEEDINGS

Norfolk, Virginia
June 14, 2016

BEFORE: THE HONORABLE HENRY COKE MORGAN, JR.
United States District Judge

APPEARANCES:

UNITED STATES ATTORNEY'S OFFICE
By: Kaitlin C. Gratton
Jay V. Prabhu
Assistant United States Attorneys
Counsel for the United States

FEDERAL PUBLIC DEFENDER'S OFFICE
By: Andrew W. Grindrod
Assistant Federal Public Defender
Counsel for the Defendant

I N D E X

E X H I B I T S

(The proceedings commenced at 12:04 p.m. as follows:)

THE CLERK: Criminal Case No. 4:16cr16, the United States of America v. Edward Joseph Matish, III.

Ms. Gratton, Mr. Prabhu, are you ready to proceed for the government?

MS. GRATTON: The government is ready to proceed.

Good afternoon, Your Honor.

THE COURT: Good afternoon.

THE CLERK: Mr. Grindrod, is your client ready to proceed?

MR. GRINDROD: Mr. Matish is ready to proceed.

Good afternoon, Your Honor.

THE COURT: All right. We're here on the defendant's discovery motion. Does either side have any evidence to present, or just argument?

MS. GRATTON: The government is prepared to present brief testimony from Agent Alfin in response to the most recently filed declaration, if the Court would find it helpful.

THE COURT: Do you have any evidence?

MR. GRINDROD: Not that hasn't been already submitted, Your Honor.

THE COURT: By that you mean the declaration?

MR. GRINDROD: That's correct, Your Honor.

THE COURT: Okay. Well, do you have any evidence?

MS. GRATTON: If the Court would permit, we would briefly call Agent Alfin to the stand.

THE COURT: All right.

(The clerk administered the oath.)

DANIEL ALFIN, called as a witness, having been first duly sworn, testified as follows:

DIRECT EXAMINATION

BY MS. GRATTON:

Q. Good afternoon. Can you please introduce yourself to the Court?

A. My name is Daniel Alfin. I am a Special Agent with the FBI. I am currently assigned to FBI Headquarters, Criminal Investigative Division, Violent Crimes Against Children Section, Major Case Coordination Unit, located in Lithicum, Maryland.

Q. And you're familiar with the case involving Edward Matish, III?

A. I am.

Q. And you've testified previously with respect to the motions to suppress the NIT warrant.

A. I have.

Q. You also submitted a witness declaration in response to the motion to compel discovery for which we are here today.

A. That's correct, I've submitted a declaration.

Q. Have you reviewed the other declaration submitted by the defendant in support of his motion to compel?
A. I have.
Q. Including, most recently, the declaration submitted of Dr. Christopher Soghoian?
A. Yes, I have.
THE COURT: Dr. who, now? Oh, the most recent one?
MS. GRATTON: The most recent declaration.
THE COURT: Right.
BY MS. GRATTON:
Q. Before we move into that, can you briefly remind the Court -- the Court is obviously familiar with the network investigative technique, but the nature of the information collected by the operation of that technique in this case?
A. The information collected by the network investigative technique was a limited set of information originating from the computer of Mr. Matish. That information was authorized by a search warrant in the Eastern District of Virginia. The information that was collected was within the scope of that search warrant.
Additionally, all the information that was collected has been provided to defense for review or has been made available to defense for review.
Q. And that includes the MAC address?
A. Correct, it included the MAC address of the computer, the

operating system version --

THE COURT: The what kind of address?

THE WITNESS: Your Honor, in order to connect to the Internet or any network, a computer has a network card in it. It could be a wireless network card, or it could be a hard-wired network card that you plug a cable into. All of these network cards, regardless of the type, have a MAC address.

THE COURT: A MAC address?

THE WITNESS: Yes, Your Honor. MAC is an acronym that stands for media address control.

THE COURT: Is that different than IP address?

THE WITNESS: Yes, Your Honor. A MAC address is unique and does not change. So you can look at the MAC address in the matter at hand from Mr. Matish's computer, and that MAC address is always the same. It is the one that was identified by the government. It was also the one that was seized by the government. A MAC address is hard-wired or burned into the card.

THE COURT: And the MAC address was among the information seized, in addition to the IP address?

THE WITNESS: Yes, Your Honor, also listed in the warrant attachment.

THE COURT: Okay.

BY MS. GRATTON:

Q. And also the operating system?
A. Correct, the version of the operating system that was active on the computer, the name of the computer itself, and the user name that was currently logged in to the computer.
Q. And all of those items were listed in Attachment B of the search warrant?
A. Yes, in one of the attachments to the search warrant.
Q. Is there other information related to the user account on the Playpen Web site? As part of the investigation, was that information maintained?
A. Yes, during the course of the investigation the FBI monitored the activity on the Playpen Web site and captured the activity associated with each individual user on the Playpen Web site. In the matter at hand that involved information pertaining to the user account on the Playpen Web site named Broden. That information was collected by the government as it was monitoring the Web site. It was not collected as a function of the NIT.
Q. Are you familiar with the information --
THE COURT: Now, wait a minute. The information about the Broden account was obtained from the Web site -- what Web site?
THE WITNESS: Your Honor, the FBI, for a limited period of time, operated the Playpen Web site.
THE COURT: Right.

THE WITNESS: Which is the Web site the defendant is accused of accessing. While we were operating the Web site we were also monitoring and recording every action that every user took on the Web site, so we were able to see for the matter at hand -- for the Broden account we can see every time the Broden account logged in, we can see where they went on the Web site, we can see what posts they accessed on the Web site, and we have a report that we've made available to defense so they can see every individual action, broken down by date and time, that the Broden user took on the Web site.

THE COURT: But you didn't know who the Broden account was at that time. Is that right?

THE WITNESS: Correct, Your Honor. That information was collected independent of the NIT.

THE COURT: Before the NIT was --

THE WITNESS: Both before, during, and after.

THE COURT: Well, but you had -- you were able to see the activity of the Broden account without having to activate the NIT.

THE WITNESS: That is correct.

THE COURT: How did you do that?

THE WITNESS: Because we had control of the Web site, we could see where all the users were going on the Web site. Even without being able to fully identify them, we could still see what the Broden --

THE COURT: So in order to find out who Broden was you had to employ the NIT. Is that correct?

THE WITNESS: That's correct, Your Honor.

THE COURT: Which you did.

THE WITNESS: That's correct, Your Honor.

THE COURT: Okay.

BY MS. GRATTON:

Q. Are you familiar with the information that has been disclosed in discovery or made available in this case?

A. I am.

Q. Can you briefly summarize that for the Court?

A. Several pieces of evidence have either been turned over to defense or made available for defense to review. One of those pieces of evidence is the activity that we monitored and collected on the Web site. That's the activity that shows when the Broden user account logged in to the Web site, where the Broden user account went to on the Web site, every post that the Broden user account accessed while the FBI was monitoring the Web site.

In addition to that, we also have turned over to defense the source code for the NIT, for the network investigative technique, that collected the limited amount of information from Mr. Matish's computer. That source code has been turned over to the defense for review. The important thing about that source code is that it can be observed,

analyzed, and it can be executed to confirm that it collects exactly what the FBI says it collects. And, additionally, it can be executed and viewed to confirm that the information that the FBI collected and made available in discovery did, in fact, originate from Mr. Matish's computer.

Q. And what would that process involve?

A. What we turned over is the source code for the NIT. And, so, Mr. Matish or a defense expert would take that code and compile it, which means just turning it into a program that you can run on a computer.

And, so, if I were the defense expert, if I was going to verify the address of the NIT, I would take that source code, I would compile it, and because Mr. Matish's computer is available for defense to review, they can actually execute the NIT on a copy of Mr. Matish's computer and confirm that it does exactly what the FBI says it does, no more than what the FBI says it does, and that the information that it collects is what was turned over in discovery and is true and accurate. They have everything that they need in order to complete that process.

Q. Was there additional information related to the transmission of data from the NIT to the government when it was executed in this case that's been made available?

A. Yes. When the NIT was executed and ran the instructions that it was authorized to run on Mr. Matish's computer, it

transmitted items of evidence to the government. Those items are what is listed in the attachments to the NIT search warrant, and that data stream was collected and preserved in its entirety. It can be reviewed. I have reviewed it myself. I have confirmed that the information in that data stream matches exactly what has been turned over to defense. It matches exactly what the FBI was authorized to collect.

Importantly, it can be reviewed. It can be used in conjunction with the source code that we've turned over to verify that what the NIT generates is the same as what the FBI has collected and turned over.

Q. And that was something that you provided this morning and are aware has been turned over to defense counsel?

A. Correct, it was provided on a disk today.

THE COURT: When?

THE WITNESS: Just before the hearing, Your Honor.

THE COURT: What hearing?

THE WITNESS: This hearing, Your Honor.

THE COURT: I thought you had already done that. You just did it today?

THE WITNESS: We turned over the source code for the NIT previously, Your Honor. What we turned over today is the copy of the network data that went from Mr. Matish's computer to the government. It reflects the same information --

THE COURT: In response to the NIT?

THE WITNESS: Yes, Your Honor.

THE COURT: All right.

BY MS. GRATTON:

Q. And you've testified that computers have been made available. Are you familiar with any reports generated based on the analysis of those computers at various times in this investigation?

A. Yes, I read reports from a preview of Mr. Matish's computer. That preview confirmed that the computer on which the NIT was executed is, in fact, Mr. Matish's computer. The information in that report matches what the FBI collected, it matches what the FBI turned over, and it matches what defense is able to duplicate with the discovery that they've been provided.

Q. And when was that preview conducted?

A. That preview, I was informed, was conducted pursuant to the search warrant that was executed at Mr. Matish's residence.

Q. And of the information that you described, can you briefly explain for the Court how it could be used to determine the full extent of what information was seized through the operation of the NIT?

A. The NIT source code that was turned over can be executed by defense. They can see exactly what information it collects, what it generates, and they can compare that to

what has been turned over to the government. If they were to execute it on Mr. Matish's computer, they would observe that the information that is collected is, in fact, what the FBI collected pursuant to the NIT search warrant.

Q. Would that process also reveal whether any additional information, such as images or other content, were transmitted as part of the NIT?

A. It would. If you were to execute the NIT, compile the source code, and run it on the computer, you would be able to observe if any images or other files were being pulled from somewhere else on the Internet. That is not a function of the NIT, but the discovery that we provided can confirm that.

Additionally, because we provided the full and not redacted data stream as a result of the execution of the NIT, that data stream can be reviewed, and it can confirm that there were no images transmitted, or videos, or any other files as a result of the NIT.

I have reviewed the data stream myself and confirmed that no files of any sort were transferred to Mr. Matish's computer as a result of the NIT.

Q. How could the information provided or made available to the defendant be used to determine whether the NIT interfered with or compromised any data or computer functions?

A. In declarations that have been submitted on behalf of Mr. Matish there are allegations that the NIT could have

installed software or could have made changes to the computer. The NIT did not install software, it did not make changes to the computer; however, defense has everything that they need to verify these claims. They have the NIT itself that they can review to confirm that it does not make changes to the computer. They also have access to Mr. Matish's computer. They can review it, they can analyze it, and they can see if there's anything on the computer, any settings that were changed or anything else as a result of the NIT.

Again, the NIT did not do anything outside of the scope of what the NIT warrant authorized; however, Mr. Matish has all the information that he needs available to him to confirm or dispute those claims.

Q. And what about determining the accuracy of the information that the NIT generated?

A. In one of the declarations that was submitted on behalf of Mr. Matish by Dr. Soghoian, it is alleged that because the NIT sent data over the regular Internet and not encrypted that the authenticity of the data could not be verified. This is incorrect.

It also fails to acknowledge that the NIT was, in fact, sent to Mr. Matish's computer over the Tor network, which is encrypted.

It also included with it a unique identifier. And, so, because that unique identifier was sent to Mr. Matish's

computer over an encrypted connection, we know that it was not tampered with at that point in time. Additionally, the transmission that was received from the government contained that same unique identifier, so the government was able to confirm when it received the information generated by the NIT that it had not been tampered with.

Additionally, in order for an individual to have successfully tampered with the NIT data stream, that individual would have had to have known about the FBI's operation, known the IP address that the FBI was utilizing. They also would have had to have physical access or some other kind of access to Mr. Matish's computer to learn the MAC address and other information from his computer. They would have had to have known that Mr. Matish was a member of the Playpen Web site, they would have had to have known when Mr. Matish was going to access the Playpen Web site, and they would have had to have a capability to intercept the FBI data stream and alter it in the course of about a second, because that's how long the NIT data stream took to transfer.

No such individual or organization exists who could have known those things and would have had the capability to alter the data in that manner.

Q. On that point, for example, when did the FBI's operation become public?

A. FBI's operation was conducted approximately between

February 20, 2015, and March 4, 2015. The first public reporting on the operation, I believe, was approximately June of that year, several months after the FBI's operation had concluded, and there is no information or evidence to suggest that anyone knew about the FBI's operation while it was ongoing.

THE COURT: Did you say from February 20th to March 4th?

THE WITNESS: Yes, Your Honor.

THE COURT: Of '15?

THE WITNESS: Yes, Your Honor.

BY MS. GRATTON:

Q. Would encryption of the data as it was transmitted from the computer to the government -- what effect, if any, would that have had on the utility of the data going forward?

A. It would have not completely made the network data useless, but it would have hurt it from an evidentiary standpoint.

Because the FBI collected the data in a clear text, unencrypted format, it shows the communication directly from Mr. Matish's computer to the government. It can be read; it can be analyzed. It was collected and provided to defense today, and they can review exactly what the FBI collected.

Had it been encrypted, it would not have been of the same value, because the encrypted data stream itself could

not be read. In order to read that encrypted data stream, it would have to first be decrypted by the government, which would fundamentally alter the data. It would still be valid, it still would have been accurate data; however, it would not have been as forensically sound as being able to turn over exactly what the government collected.

Q. And on the question of chain of custody, that data stream includes the unique identifier?

A. Correct. The chain of custody of the evidence is valid, the digital chain of custody, as it's referred to. Because the data stream included a unique identifier, that unique identifier was sent to Mr. Matish's computer over the encrypted Tor network. It came back with the NIT results. It was not changed in transit, and it did, in fact, report accurate data from Mr. Matish's computer.

And more important is the fact that the defense does not have to take the government's word for it. They have all the tools that they need to recreate exactly what the government used by using the NIT source code, comparing it to the network packet capture, and comparing it to the data that was provided in discovery. The defense has everything they need to recreate every step of this process to validate the data that we have provided.

Q. And when you say that the data was accurate, have you reviewed information from the computer seized in this case

and compared it to the NIT results?
A. I have. I have reviewed that data and confirmed that the information that the NIT collected does in fact match information from Mr. Matish's computer.
THE COURT: How much longer do you expect your brief evidence to take?
MS. GRATTON: If I may just have five more minutes, Your Honor.
THE COURT: All right.
BY MS. GRATTON:
Q. Have you reviewed the unique identifiers generated through the operation of the NIT in all cases such as this?
A. Yes, I've confirmed that every unique identifier that was generated in this investigation was, in fact, unique. There were no duplicate identifiers generated.
Q. Would a disclosure of -- well, have you reviewed the charges pending in the superseding indictment in this case?
A. I have.
Q. Are any of them tied to child pornography found on Mr. Matish's computer?
A. No. The charges in the matter at hand stem from the activity of the Broden user account on the Playpen Web site, which is corroborated by statements made by the defendant.
Q. Are you aware of whether child pornography was, in fact, found on any of these devices?

A. I have been informed that child pornography was found on devices belonging to Mr. Matish.
Q. Where?
A. It was found in unallocated space on his computer, and what that means is the images of child pornography were placed on his computer at some point in time and then deleted. The FBI was able to recover them using forensic software.
Q. Would there be any information in files found in that location regarding their source or when they were placed on the computer?
A. No.
Q. Would any further disclosure of information related to how the NIT was executed reveal where that information came from?
A. There is nothing else in the government's possession that could shed light on where the images of child pornography on Mr. Matish's computer came from.
Q. Did the NIT have any other functionality beyond that described in the warrant, such as turning on webcams?
A. No. The functionality of the NIT was described very specifically in the NIT warrant. It did not have any functions outside of what was described in the NIT warrant. It did not install any software, it could not remotely take control of the computer, there was nothing left behind. No

settings on the computer were altered.
Q. And could that be verified through a review of the NIT code and the computer as you've testified and as described in the declaration?
A. Yes.
Q. Have you performed such reviews in the past in other cases?
A. I have in other cases conducted analyses of computers that were thought to be infected with either malware or viruses or other software. I have conducted that review on my own. I have been successful in finding such malware and analyzing it.

Mr. Matish has everything available to him to conduct such an analysis, should he decide to do so.
Q. And the process for that is described in the declaration you submitted to the Court?
A. That's correct.
Q. And, finally, would you describe the NIT as malware?
A. No. The declaration of Dr. Soghoian disputes my point from my declaration that I do not believe the NIT should be considered malware, but he fails to address the important word that makes up malware, which is "malicious."

"Malicious" in criminal proceedings and in the legal world has very direct implications, and a reasonable person or society would not interpret the actions taken by a law

enforcement officer pursuant to a court order to be malicious. And for that reason I do not believe that the NIT utilized in this case pursuant to a court order should be considered to be malware.

Q. Would it have fundamentally altered the defendant's computer?

A. No, and the defendant has everything he needs available to him to dispute that claim. There's nothing to dispute, but he can try to if he wants to. He has his computer available to him. He also has the NIT available to him to review.

Q. Thank you.

MS. GRATTON: Would you please answer any questions that the defense or the Court may have.

MR. GRINDROD: May I inquire, Your Honor?

THE COURT: You may.

CROSS-EXAMINATION

BY MR. GRINDROD:

Q. Agent Alfin, I'm going to jump around a little bit. I'll try to let you know where I'm going.

So you started off talking about various items of evidence that have been made available to the defense.

A. Yes.

Q. Now, you're aware that the defense requested all this information about the NIT and the code and the computer

programming back in March, right?
A. I don't know the exact date, but I'm aware that these requests have been made.
Q. Okay. And you talked about the fact that the government made available the source code for the NIT, which has been referred to also -- we refer to it as the payload.
Do you know what I'm talking about?
A. The defense has. You have referred to it in different terms. We have turned over what the government has defined as the NIT in its entirety.
Q. Okay. And you're aware that the first time that the government agreed to produce that particular data was in its response to this motion to compel?
A. I assume that's the case. I don't know exactly what date it was provided on, but I know it was turned over.
Q. And then you talked about a data stream being made available, right?
A. Yes.
Q. And you're aware that the first time that the government agreed to produce that data was in its surreply to the motion to compel.
A. I don't recall the first time that that data was made available, but I know it has been made available and has been turned over.
Q. As of --

A. As of today.
Q. -- 20 minutes ago, correct?
A. Yes. To the best of my knowledge, it was not turned over prior to that.
Q. And you talked about access to Mr. Matish's computer itself being, perhaps, a substitute for some of the other data that the defense is requesting, right?
A. Everything that the defense has requested can be verified with the discovery that is available.
Q. Now, the problem with that, right, is that a computer is a malleable object, right, from a data perspective, right?
A. Data on a computer can change.
Q. And, so, there are a number of sophisticated forensic techniques for recovering data from computers, right?
A. There are.
Q. But, at bottom, once a particular bit, once a particular data point is written over, it's gone forever, right?
A. After data has been overwritten it can be very difficult or impossible to recover, yes.
Q. Okay. And so the NIT in this case, the exploit, was deployed in February, right?
A. I believe it was in February, yes.
Q. And law enforcement did not actually go and seize Mr. Matish's computer until much later that summer, and I believe it was July, right?

A. I don't remember the exact date, but, that's correct, I believe it was several months later.
Q. So there's a significant time gap between when the government ran its exploit, right, broke into Mr. Matish's computer, and when it actually physically went and seized the computer, right?
A. There was a period of several months in between the NIT identifying Mr. Matish and the search warrant that was executed at his residence, yes.
Q. Okay. So if the government's use of the exploit made Mr. Matish's computer vulnerable to some sort of other malware attack -- right? -- then that evidence may have existed on the computer at some point during that months-long period but may not exist now, based on the computer as recovered in July, right?
A. The defense has said in its declaration that the NIT may have made fundamental changes to Mr. Matish's computer; however, the preview reports that I have read that are also available to defense review show that the important information on the computer remained the same between the time that the NIT identified his computer and the time that the search warrant was executed.

Additionally, it's my understanding the defense has made no effort to actually analyze his computer to search for any fundamental changes or any other alterations to the

computer that are alleged.
Q. Okay. So my question was if there was some malware or someone exploited the vulnerability created by the FBI in February --
A. The FBI did not create any vulnerability.
Q. I want you to assume that they did for purposes of my question, okay?
A. They didn't. I can't answer your question like that.
Q. Well, you're testifying as an expert in this case, correct?
A. I don't believe I was qualified as an expert.
Q. So none --
A. I can --
Q. None of the opinions, none of the testimony you're offering in this case, is based on any sort of expertise?
A. No, it certainly is. I'm just -- for the record, I don't believe I was officially qualified as an expert. I know different districts handle that differently. I just want to make sure I'm not misrepresenting my position.
THE COURT: Well, I think when you file a declaration in response to another person's expert declaration that you're acting as an expert.
THE WITNESS: Understood. Different districts --
THE COURT: So I think that Counsel can ask you a hypothetical question which, if you are able to answer, you

should answer.

THE WITNESS: Understood, Your Honor.

THE COURT: So go ahead with your question.

MR. GRINDROD: Thank you, Your Honor.

BY MR. GRINDROD:

Q. So I'm asking you for purposes of this question to assume that the FBI did create some sort of vulnerability when it deployed the exploit in this case on Mr. Matish's computer.

A. Okay.

Q. That would have taken place back in February, correct?

A. Correct.

Q. And if that vulnerability led to some other malware or some other security breach in Mr. Matish's computer, the evidence of that breach or of that other malware may have existed on Mr. Matish's computer at some time between February and July but may have disappeared by the time the government seized that computer in July, right?

A. In this theoretical situation that describes the events, that did not happen. Data could be deleted. It's certainly possible.

Q. So the answer to my question is "yes," correct?

A. The answer to your question is that data can be deleted.

Q. And you would agree with me that when hackers or other people use malware or try to surreptitiously get onto someone's computer those programs are often designed in a way

to try to actively cover up tracks, right? They try not to leave evidence behind of the fact that they were there, right?
A. Some malware is designed with those features, yes.
Q. So...
MR. GRINDROD: The Court's indulgence, Your Honor.
(There was a pause in the proceedings.)
BY MR. GRINDROD:
Q. So let's talk about -- at various points in your direct testimony you said that if you were the defense expert you would do X, Y, or Z. Do you remember those statements?
A. Yes, I remember them.
Q. And you also testified that in your capacity as, I guess, a government expert in this case you have gone and looked at the data, the evidence itself, and analyzed it and then made some sort of conclusion or statement in your declarations or in your testimony today, right?
A. Yes, that's true.
Q. And you mentioned at various times that if you were the defense expert you would confirm that you would use the data provided to confirm that the data did what the FBI says it did, right?
A. I said that I would use the evidence that the government has provided in discovery to confirm that the evidence that we collected and made available is an accurate representation

of what the NIT actually sent from Mr. Matish's computer.
Q. You testified on direct that the use of -- that the analysis of the NIT would allow a defense expert to confirm that it does exactly what the FBI says it does.
Do you remember that testimony?
A. Yes. That, combined with the other evidence available, but, yes, I said that.
Q. And what you're saying, right, is based on the data you have provided, some data, that a defense expert, technological expert, could look at the data to determine whether, in fact, what the FBI says they did actually is what they did, right?
A. Yes, that's correct.
Q. Okay. And you would agree with me that that is a proper role for a forensic expert.
A. Yes.
Q. Okay. You would also agree with me that the government has not produced some of the data, including the exploit, in this case, correct?
A. There was an exploit used in this case that has not been turned over because it is immaterial.
Q. And you agree that it is possible for an exploit to make fundamental alterations to a computer system.
A. Yes. In my declaration I stated that an exploit -- not the one used by the government -- could make alterations to a

computer system; however, the one the government used did not.

Q. Okay. So that part of your statement, the "however" -- right? You say, "however." An exploit can do this; however yours didn't, right?

A. Correct, and that can be confirmed by analyzing Mr. Matish's computer, which is available to your defense to review.

Q. Well, except that my client's computer may not contain that data. You just testified it may have been overwritten, right?

A. It contains the same data that the NIT collected back in February. We've reviewed that report.

Q. So you would agree with me that with respect to some of the data you've agreed to produce you say a defense expert should look at the data and, based on looking at the data, they can confirm whether or not the technology actually did what the FBI says it did, right?

A. Yes, they should look at what we provided to confirm that what we've provided does what we say it does.

Q. And you would agree with me that the government, having not produced the exploit -- the defense experts cannot look at the exploit to see if the exploit did what you say it did, right?

A. The exploit, again, would shed no light on what the

government did. It would not --
Q. Let me stop you there and ask a follow-up, if I can.
A. Okay.
Q. You say the exploit would shed no light on what the government did. The government deployed this exploit, correct?
A. The government used the exploit to deploy the NIT.
Q. And I believe you used the analogy that this exploit is like a way of picking a lock, right?
A. Yes. A more accurate analogy may be going in through an open window. As I've stated in my declaration, there was a vulnerability on Mr. Matish's computer. The FBI did not create that vulnerability. That vulnerability can be thought of as an open window. So we went in through that open window, the NIT collected evidence, and then left. We made no change to the window.

Looking at that window, telling you what window it was, you can look at the window all day long. It gives you no insight into what the FBI did or what evidence was seized. In order to know that you have to analyze the NIT, which was turned over in its entirety.
Q. So let's not confuse analogies. Let's go back to the one you used in your declaration about picking the lock.
A. Okay.
Q. So you're telling us that you know exactly how the

government picked the lock on the front door to Mr. Matish's computer, right?
A. I know information about how the FBI deployed the NIT.
Q. And that's because you've seen the data that makes up the exploit, right?
A. No, I have not.
Q. So you're offering sworn statements about what the exploit did or didn't do. What is the basis for your testimony?
A. I have executed the NIT, which included utilizing the exploit on a computer under my control. I confirmed that it collected the information that it was authorized to collect, and I confirmed that it did not make any fundamental changes to my computer.
Q. So you didn't even look at the actual code, at the actual data, you just tried to observe the effects of executing the code?
A. I have not viewed the exploit myself, nor have I ever claimed to or made any implication that I have.
Q. Well, you make a number of explanations about what the exploit is and what it does and doesn't do.
A. Yes.
Q. But it's your testimony today that you've never even looked at this data that the defense is requesting.
A. You can use a computer without knowing how to build a

computer and see what the computer does.

I never claimed to have looked at the exploit, nor would there be any need to, because, again, as stated previously, it is immaterial.

MR. GRINDROD: No further questions, Your Honor.

MS. GRATTON: If I may just briefly address a couple of points, Your Honor, very briefly.

REDIRECT EXAMINATION

BY MS. GRATTON:

Q. The defense asked you about a hypothetical in which the FBI created a vulnerability. Is there a way to test whether any such vulnerability was created?

A. Yes. If they want to see if there were any fundamental changes or vulnerabilities on Mr. Matish's computer, they can review Mr. Matish's computer, which they have declined to do thus far.

Additionally, they can look at the NIT source code, which we have provided in its entirety, and confirm that it does not make any changes to the computer or open up vulnerabilities.

Q. And the information gathered by the NIT, to briefly summarize, was the operating system, the host name, the user name, the MAC address, the unique identifier, whether the NIT had been deployed to it before, and then also the IP address disclosed in the transmission of that information back to the

FBI?
A. Whether or not the NIT had been deployed to the computer previously was information tracked by the government. Mr. Matish's computer would have no way of knowing that itself, but, yes, those are the items listed from the warrant attachment.
Q. Are any of those items -- I believe you testified to the MAC address. Can that be changed?
A. It can be --
MR. GRINDROD: Objection, Your Honor. This is all outside the scope and asked and answered.
MS. GRATTON: Your Honor, the defense is arguing that some hypothetical attack on Mr. Matish's computer through a hypothetical vulnerability resulted in significant changes to his computer that may no longer exist, and, so, I'm trying to determine whether the information at issue, which are the items collected by the NIT, could have been changed.
There's been testimony that they did not change, but whether a MAC address or an operating system is subject to complete hack and overwritten, that may have vanished in the months between the execution of the NIT and the seizure of the defendant's computer, as Counsel suggested on cross.
THE COURT: Well, I think he's already answered that question.

MS. GRATTON: Very well.

BY MS. GRATTON:

Q. And although you've not reviewed the exploit source code, are you familiar with the operation of the NIT in this case?

A. I am.

Q. And you --

MS. GRATTON: No further questions.

THE COURT: All right. You may step down.

THE WITNESS: Thank you, Your Honor.

THE COURT: All right, Mr. Grindrod. It's your motion, so I'll hear first from you.

MR. GRINDROD: Your Honor, I would first direct the Court's attention to the decision in *Michaud*, which since the last time we were here I've supplemented the record with the order from that case that addressed the discoverability of this same information and the transcript regarding the same --

THE COURT: You did, but it didn't really give any reason for the opinion.

MR. GRINDROD: Well, Your Honor --

THE COURT: It just said he had studied it before and mentioned a series of amendments and said, that's it.

MR. GRINDROD: Well, Your Honor, I would just note --

THE COURT: So the decision is helpful, but the

rationale is absent.

MR. GRINDROD: I understand the Court's position.

The Court in that case did rely on expert declarations that were very similar to and in some cases drafted by the same experts in this case, which I do think is probative, but I understand the Court's position on that.

I would also note the government raises in its surreply that there is some meaningful difference in the circuit standard. I think that's a bit of a red herring, Your Honor. Under either the Ninth Circuit standard or the Fourth Circuit standard, which we agree is set out in *Caro*, there is a strong indication that this evidence will play a role in uncovering admissible evidence, aiding in witness testimony, and corroboration and/or impeachment.

Your Honor, I'm going to use a couple of analogies, because I think it's important not to get too lost in the weeds of the technology here. But I think it's appropriate to view this code as analogous in some ways to a confidential informant or the underlying DNA analysis that we see in maybe a more common case. And the fundamental disagreement between the government and the defense in this case is whether the defense is entitled to the evidence or, alternatively, whether the defense is entitled to the government's description of or assurances about what the evidence will show.

It's our position, Your Honor, that the government cannot simply say, we've reviewed the evidence, or, in the case of Agent Alfin, I haven't actually looked at the code that you want, but I can still tell you you don't need it.

We've set out through our expert declarations exactly why this information is critical, and the government is saying, no, we've looked at it, we've analyzed it; our experts say you wouldn't be able to make a meaningful trial defense based on this information. But in some ways, Your Honor, that's the same as saying, we're not telling you who our confidential informant is. You don't need to talk to him, because we're telling you he's believable and everything he's saying is true. You don't need to look at the DNA tests from the lab, because we're telling you it's a match, and we're telling you the tests were fine.

The government has the evidence --

THE COURT: Well, now, among the things that were in your expert declaration was that you could tell -- or you wanted to examine the exploit to determine if the information sent back from the defendant's computer to the government's computer was compromised.

MR. GRINDROD: That's one reason we need the exploit. That's one reason we need that.

THE COURT: Now, what information do you have that that information was compromised in transit?

MR. GRINDROD: Well, we know, Your Honor, that it was susceptible to being tampered with, and --

THE COURT: Why? How do you know that?

MR. GRINDROD: Well, that's based on Agent Alfin's testimony at the suppression hearing. We know that this information was not sent in encrypted form, and Dr. Soghoian sets out in his declaration that that's very important, because when information is sent through unencrypted channels it's particularly susceptible to being tampered with. So that's one reason, Your Honor.

But the other reason, Your Honor --

THE COURT: Well, they also said that the best practices required that it be encrypted.

MR. GRINDROD: That's what our expert would say, Your Honor, yes -- or has said.

THE COURT: Why would that be the case?

MR. GRINDROD: To prevent tampering with the evidence. I mean, this is analogous to -- I mean, there's a crime scene. Certain evidence is collected, and rather than bagging and labeling it and following established techniques for how evidence is to be collected and transferred back to, you know, the server, which is like an evidence locker, they just threw everything in the back seat of the cruiser and drove back. Oh, and, by the way, they won't tell us whether on the way back they also picked up someone else who rode in

the back of the cruiser.

I mean, in some ways the government is right that by maintaining a monopoly on the evidence, by keeping the evidence secret from the defense, we can't, with absolute certainty, say that the evidence was tampered with. We can just say that we know, based on Agent Alfin's declaration, that it was susceptible to being tampered with and that the evidence of the government --

THE COURT: Well, your experts seemed to indicate that they thought it could be tampered with as well.

MR. GRINDROD: That's correct, Your Honor.

THE COURT: And, therefore, it should have been encrypted.

MR. GRINDROD: That's correct, Your Honor.

THE COURT: Because if you don't encrypt it, anybody can tamper with it.

MR. GRINDROD: I think that's correct, Your Honor.

And, also, I think the exploit is particularly important here, Your Honor. And the government concedes that an exploit -- although, they don't say theirs did this -- that an exploit can create critical vulnerabilities, make fundamental changes to a computer system. And Agent Alfin somehow, without having actually looked at the code, is able to offer under-oath statements that their exploit did not do those things. But, again, this notion of unlocking --

THE COURT: Your experts have not examined the defendant's computer.

MR. GRINDROD: That's correct, Your Honor.

THE COURT: But the government has offered them the opportunity to do that.

MR. GRINDROD: That's correct, Your Honor, and we've actually very recently had some conversations about getting a forensic copy of the computer to better analyze the parts of the code that the government has produced. But we don't agree that that's a substitute, I mean, for the very reasons that Agent Alfin said on the stand; that there was --

THE COURT: Well, if you examined the defendant's computer and hypothesized there had been some malware inserted on the computer in this gap period you're talking about, maybe it would still be on there, and maybe your experts could find it.

MR. GRINDROD: That's true, maybe, but --

THE COURT: Oh, well, "maybe's" are what we're talking about here, because maybe there's malware on it, and maybe they could have found it, if there was. So it would seem --

MR. GRINDROD: But what's critical -- sorry, Your Honor.

THE COURT: Don't talk over me.

MR. GRINDROD: Yes, Your Honor.

THE COURT: It seems to me that by examining the computer they would have had everything to gain and nothing to lose. They might have found something that would give them a factual basis for saying that they need the source code. Maybe they would; maybe they wouldn't. But if they did, it would certainly strengthen their position in asking for the code, wouldn't it?

MR. GRINDROD: I think that's probably right, Your Honor.

THE COURT: All right. Well, I don't understand why they wouldn't have taken advantage of that opportunity before today's hearing.

MR. GRINDROD: Well, Your Honor, it's unlikely that -- I mean, Agent Alfin touched on this, but, I mean, the malware that would have taken advantage of the vulnerability that may have been created by the government is, in all likelihood, designed not to be found, and, so, the fact that --

THE COURT: I think what I'm saying is they had everything to gain by examining the computer and nothing to lose. What could they have lost by examining it?

MR. GRINDROD: Well, a lot of money. But, I mean, Your Honor, the fact of the matter is that --

THE COURT: Well, you haven't asked for any money to cover their cost of examining the computer, have you?

MR. GRINDROD: No, Your Honor, but if the government wants to pay for our expert to conduct a full forensic analysis and then, if and when they don't find anything, they'll agree to produce the exploit, then we would agree to that process. I mean, the fact that --

THE COURT: Well, I don't understand why they wouldn't do that, because they've got everything to gain and nothing to lose by examining his computer. I mean, they might find -- they said, well, maybe there was another source for the pornography other than directly from Playpen.

Well, if they examined the computer maybe they would find some evidence that there was some other source. Maybe they would; maybe they wouldn't. But, again, isn't it worth a try?

MR. GRINDROD: Well, perhaps it is, Your Honor. I would say that --

THE COURT: And shouldn't they try before they come here and ask for the source code?

MR. GRINDROD: No, Your Honor, and let me explain.

THE COURT: Why not?

MR. GRINDROD: Well, because --

THE COURT: Because then there might be some basis in fact for them to believe that they might find something.

MR. GRINDROD: Well, there is a basis in fact to believe that --

THE COURT: No, I think at this point it's very speculative.

MR. GRINDROD: Well, if our experts analyzed the computer and they found nothing, then the exact points that they've made today are exactly the same.

If they have the exploit, that also could help them look for --

THE COURT: Well, I mean, if they examined it and there was no evidence of anything on there in the way of malware and there was no evidence that there was any breach or change to the security apparatus on the computer, it would weaken their case in asking for the source code, wouldn't it?

MR. GRINDROD: No, Your Honor.

THE COURT: It wouldn't?

MR. GRINDROD: And that's the point I'm trying to make.

So the absence of finding malware on the computer itself is the expected outcome, even if there was malware on the computer, and, so, what we need to do --

THE COURT: Well, it sounds to me like, then, that they're saying that there's not much probability that there's anything on there.

MR. GRINDROD: Again, I disagree with that characterization, Your Honor. I think that what they're saying is that the --

THE COURT: I think what they're saying is they want to call it -- they want to call NIT malware.

MR. GRINDROD: I don't think that matters at all, Your Honor.

THE COURT: Absolutely. I one hundred percent agree with you. So why are they doing it?

MR. GRINDROD: Well, I think the academics get excited about it, Your Honor. I think there's still a --

THE COURT: I think the academics don't like what the NIT does.

MR. GRINDROD: They may or may not, but I think, from the perspective of this case, whether you call it malware or not is rhetorical, at best. The fact is --

THE COURT: I agree with you, but if that's the case why have they spent so much time trying to say it's malware? Because they try to say it's malware, and it seems like in saying that they're implying that they don't think the government should have this capability.

MR. GRINDROD: I think that's a normative question that the experts in this case don't have to reach. Perhaps Congress --

THE COURT: Well, they seem to have been trying to reach it whether they need to or not.

MR. GRINDROD: I agree that there are probably some definitional points in this case that are, perhaps,

technically important, but for the Court's purposes in deciding this motion I don't think need to be resolved one way or the other.

For example, whether we call this what the government is requesting, the full source code or the payload, or -- I mean, everybody now knows what we're talking about.

THE COURT: Exactly, and I don't think the labels -- no, I agree with you on that. I think labeling it is an exercise in uselessness, but it's interesting that they spend so much time trying to so label it.

MR. GRINDROD: Well, I think, Your Honor, as long as -- I mean, at some point the definitions are only important for getting everybody on the same page. And I think, despite some initial confusion, everybody at least now has a generalized understanding of what exactly it is the defense wants, what the government won't produce.

And I would agree with the Court that, for today's purposes, what we call it is probably less important. But the evidence is still critically important, and that's what we're asking for, Your Honor, is that the government -- this notion of picking the lock to the front door of Mr. Matish's computer is, I think, one that Agent Alfin put forward and one that is particularly well-suited to demonstrating why we need this information.

Agent Alfin suggests, without having looked at the data, that this particular exploit worked in a way where the lock was picked but then, after the FBI left the computer, the door was locked behind it; there was no vulnerability created. But he agrees, and our experts have set forward a basis, that without looking at the code there's no way to know whether the door was locked after the FBI left or whether it was just left unlocked or that the front door was open so that anyone passing by could walk right in, and it was obviously kind of advertising the software vulnerability.

But all of those things are questions that can only be answered if we have the data, and the government not only refuses to produce the data but refuses to put on any evidence by anyone who has actually looked at the data. I mean, they initiated this prosecution based on this technology, and now they're playing hide-the-ball. And, Your Honor, I mean, it goes to the fundamental fairness of the prosecution. If the government is going to initiate a technology --

THE COURT: Well, of course, the problem is that the evidence indicates -- or one of the problems is that the evidence indicates that the defendant entered the Playpen site before the NIT was instituted.

MR. GRINDROD: I think that's the government's position, Your Honor.

THE COURT: Yes, well, that's it, and I think the defendant admitted that in a written statement which the Court has ruled is admissible. So what you're trying to do is say, if we got the source code, we could prove that what the defendant admitted to is wrong.

MR. GRINDROD: What we're saying, Your Honor, is that whatever evidence the government may have against our client, he's entitled to a defense under the Constitution. And the defense we propose to mount is one that is, in part, at least, based on a technological defense to the government's technological evidence. And the only way we're going to be able to mount that defense is to have an expert to counter the inevitable government expert who is going to talk about how reliable this NIT was and how it worked and how it didn't make any fundamental changes to our client's computer. You know, how is Mr. Matish supposed to challenge that evidence or test that evidence? This is the adversarial system in which --

THE COURT: Step one should have been examining his computer, as the government points out in its brief.

MR. GRINDROD: Your Honor --

THE COURT: And that's -- and I haven't heard any reason why they didn't do that. And the witnesses have elected to testify by declaration so that they couldn't be cross-examined, which is an interesting way of presenting

their evidence, but that's the way you've chosen to present their evidence. So these questions that the Court has, they're not here to answer them, so the Court has to draw inferences from what they've done and what they have failed to do.

MR. GRINDROD: Well, Your Honor, the experts have not conducted a forensic analysis of the computer because they haven't been directed to do so by counsel.

THE COURT: Well, it seems to me that they should have directed counsel that that's what should have been done. Counsel is not the expert on the computer. Counsel shouldn't have directed them to search the computer, they should have directed counsel that the computer should have been searched.

MR. GRINDROD: And, Your Honor, if that was the appropriate step, then I believe they would have. And that's my point, Your Honor. I mean, I get that there's some rhetorical appeal to this notion of looking at the computer.

THE COURT: Well, they didn't do it.

MR. GRINDROD: Because --

THE COURT: And what they failed to do speaks very loudly.

MR. GRINDROD: Well, Your Honor, again, I mean, I think that's only -- that's only -- there's no -- if they looked at the computer, no matter what they found, the answer is we still need the exploit.

THE COURT: If they looked at the computer, perhaps there's evidence there indicating that what they say may have happened is a bit more likely to have happened, if they looked at the computer and found something to support their hypotheses. And I think it's a generous term to describe it as a hypothesis. It could just as well be described as speculation.

And they could have -- the evidence is perhaps there for them to have found some lead on the computer. Experts can do amazing things with computers. I remember the case where the man took the computer from his place of employment and put something on there that was called Erase to erase all his e-mails. And then he took it to the junkyard and beat it with a sledgehammer. And then it was recovered, and they got information off of the computer as to his e-mails.

Experts can get a lot off of computers, and I'm at a total loss to understand why they didn't instruct you that that should be done.

MR. GRINDROD: Your Honor, I've raised that point with Dr. Miller, specifically, and the answer is because it doesn't move the ball forward. I mean, we can spend a bunch of money --

THE COURT: Well, I think the answer may be that Dr. Miller is more interested in getting the code than getting the information.

MR. GRINDROD: I don't know that there's any basis for that, Your Honor. I mean, he's subject to a protective order. It's not like he can publish based on any information that he gained as a result of this.

THE COURT: I think one of your experts has already published based on information he gained from this sort of situation, hasn't he?

MR. GRINDROD: I'm not -- I'm not aware of that, Your Honor. I know Dr. Soghoian has not reviewed any information that's subject to the protective order in this case, so I don't believe he would be --

THE COURT: Well, it's clear -- if nothing else is clear, it's clear that the experts don't like the fact that the government has this device at their disposal. That's absolutely clear.

MR. GRINDROD: But these are accomplished academics, Your Honor, from --

THE COURT: They're hired experts. And the fact that you have two of them doesn't add to their credibility, because, quite frankly, you could probably find any number of them, if you wanted to, who would say the same thing. It's like Tweedledum and Tweedledee; oh, yes, I agree with Dr. So-and-so's analysis. Well, I didn't expect him to say that he disagreed with it, because if he did I don't think I would be looking at his declaration.

MR. GRINDROD: The government's only expert in this case is their case agent, who is running this whole operation. I mean, this is Agent Alfin's show, with hundreds of prosecutions across the country. I don't know that his -- I mean, the Court can evaluate the credibility of the various experts, but the testimony of someone who is the lead case agent --

THE COURT: I mean, are you saying that an expert who part of his job is being an expert and is not paid anything extra is to be criticized for that, as opposed to somebody who is hired to say something?

MR. GRINDROD: Dr. Soghoian is doing this pro bono, as he states in his declaration.

THE COURT: Well, I guess Agent Alfin is doing it pro bono, too, because he gets his regular salary. He's not getting paid extra for being an expert, is he? You can ask him that, if he's getting paid extra. I guess your guy who is doing it pro bono is getting a salary, isn't he?

MR. GRINDROD: Your Honor, I'll leave it to the Court to decide whether Agent Alfin has a stake in the outcome or --

THE COURT: Well, let's not -- okay.

MR. GRINDROD: Thank you, Your Honor.

MS. GRATTON: Thank you, Your Honor.

I think, as the Court has pointed out in questioning

the facts and whether we're dealing with facts or speculation, really gets to the heart of the issue here, which is whether the information sought is material, which is the standard under Rule 16. You know, if the inquiry is whether it's material, if it's material, is it subject to privilege, which the government has asserted, and, if so, whether there's been a compelling need shown sufficient to overcome that privilege.

But on the question of materiality, the defense has cited a number of purposes for which he claims he needs the information, including the full extent of the information seized by the NIT, whether it interfered or compromised any computer data functions, whether it was accurately described, the chain of custody, and then the source of the child pornography found on his computer.

THE COURT: Well, it's his job to challenge everything, isn't it?

MS. GRATTON: Yes, of course. I just -- in looking at the reasons stated for disclosure of what is, essentially, how the NIT got to his computer. Because he has the computer instructions that generated the results. He was provided today a copy of the data stream that shows exactly how those results were transmitted back to the government. And, as Agent Alfin testified, he has, with that information, coupled with the --

THE COURT: Well, he doesn't want to believe what they say. Is he entitled to check his credibility by getting the source code?

MS. GRATTON: I think he first has to make a showing of materiality, which requires under *Caro* that there must be some indication that the pretrial disclosure would enable him to significantly alter the quantum of proof in his favor. And there has to be a threshold showing of the materiality of the information there, one based on facts and not speculation.

As the Court has noted, the defendant has not examined his computers. He's not pointed to anything in any of the evidence that's been disclosed or made available indicating that there's any sort of discrepancy or irregularity in what the government has done, and --

THE COURT: Does it make any difference that the defendant said that he was responsible for the Broden posting on Playpen prior to the NIT being deployed? Does that make any difference?

MS. GRATTON: The government does believe that it makes a significant difference, because --

THE COURT: Well, it wouldn't make any difference if the Court's ruling on this motion impacted the Court's ruling on the invalidity of the NIT search, to begin with, because then we wouldn't get to the confession, would we?

MS. GRATTON: If the Court were to determine --

THE COURT: Does the Court's ruling on this discovery motion impact the Court's ruling on their first motion to suppress?

MS. GRATTON: Based on the fact that the defendant has provided only speculation that the NIT did not operate in the way that the government has said that it did, or that it gathered or transmitted information beyond what's been disclosed. All of it, as outlined in the government's response and surreply, is speculation.

There's been a significant amount of evidence on this issue turned over to the defendant, and yet he doesn't point to anything in the computer instructions saying that those instructions would have done something other than what's been represented, that they would have generated results other than those disclosed, that they transmitted any information, such as images or other content.

So the government's position is that --

THE COURT: Well, the FBI could have just gotten that second warrant to cover their tracks, couldn't they? Maybe they got the images through the NIT but they realized that that went beyond the search warrant, so they went and got a second search warrant to cover their tracks. They could have done that, couldn't they?

MS. GRATTON: Well, the response is twofold. First,

there were no images transferred back to the FBI by --

THE COURT: Well, I mean, that's what they say, right. I mean, does the defendant have to believe that?

MS. GRATTON: No. He has the data stream as it was transmitted from his computer to the FBI. He can look at that to see if there was anything other than the NIT results transmitted back to --

THE COURT: Well, they're saying that if they had the source code it may show that they got something else other than --

MS. GRATTON: The source code did not collect or transmit information. As Agent Alfin testified, it allowed the FBI to enter an open window.

THE COURT: The source code allowed them to enter the open window, but it didn't play a part in the information they gathered. That's what they said. How do they test the accuracy of that information?

MS. GRATTON: The computer instructions, if they recreate those and execute them on the defendant's computer, will generate the same results. And they can test that. If they ask to review forensically the computer, they can analyze it for the presence of any malware. They can execute a copy of the NIT that's been provided and determine if it does anything other than it said it would do.

If the Court were to order, as the defendant

describes, the payloads, any and all payloads, delivered to the defendant's computer as --

THE COURT: Well, the difficulty in using language like "payloads" is everybody uses a different description, and it gets confusing to the Court reading all this --

MS. GRATTON: If the Court were to order the government to provide all the source code that gathered or transmitted information from Mr. Matish's computer to the government, I could stand here today and tell the Court that the government has already provided that information. So the exploit at issue is not -- it didn't collect, it didn't transmit information.

And the question about the child pornography found on the computer, the FBI did get a second search warrant. They got a search warrant for the residence that --

THE COURT: Well, I know they did, but maybe they did that just to cover their tracks, huh?

MS. GRATTON: The defense can review the data stream and see. The only -- again, the Court could order us to disclose the instructions that gathered or transmitted information and all transmissions from the defendant's computer, and we have disclosed those. The defense can review them and, if any such evidence exists, could highlight that for the Court.

With respect to the computer instructions, Counsel

has had those for some time. Admittedly, the network stream was produced this morning. There was -- between the two hearings counsel for both sides were out and, at the earliest time possible, discussed the production of the stream, and it was brought here today in accordance with the agreement that we reached. But the defense can analyze that and determine whether any images were sent back, whether the FBI was trying to cover its tracks by finding the image through a forensic examination of his computer after the search.

But I think the most important point about those images and one that is, perhaps, not covered as it should have been in the government's briefing is that, as testified to here today, they were in unallocated space, they had been deleted, and none of the charges against the defendant are based on anything recovered from his computer. The NIT was used to identify and locate him, as the Court is well familiar from its consideration of the first and third motions to suppress.

The child pornography on the computer does not serve as the basis for any charge, and the defense can look at the information that was collected through the NIT at various points, they can see the computer instructions, they can see the network stream of the results and the results as maintained and turned over by the government in a copy of the user report and see that all of that is the same. And not

only is that the same, but later reviews of the defendant's computer identified the same information. The preview done at the time of the search shows the same operating system, the same information, as does the later forensic report, to a certain extent. And the defense itself can go and review the information, and if it's the same at every point there's no reason to think that it was changed.

And, as Agent Alfin testified, the transition from Mr. Matish's computer to the government included a unique identifier that the FBI verified had not been changed. And he also testified about all of the things that would have to occur for any kind of tampering with that transmission to have taken place, including an extensive amount of knowledge that would have had to have been available about the FBI's investigation, both as to the FBI and the defendant, as well as the ability to intercept and manipulate the transmission in one second.

THE COURT: Well, I'm sure that if they had encrypted it and the encryption had to be translated by the FBI they'd be complaining about the translation of the encryption. But that's his job, to complain about such things.

MS. GRATTON: And that would be the government's view as well. The defendant has a number of tools to determine that the information gathered and used to identify

him is accurate.

And when considering whether further disclosure of how the NIT got to him would significantly alter the quantum of proof in his favor, the government does think the Court can look to the confession, look to the full quantum of proof of evidence available in this case to determine whether some questioning as to how information was transmitted back through the operation of the NIT would undermine the fact that the defendant acknowledged that well before its execution he was acting as Broden on the Playpen Web site. So the government does think that that fact is significant when determining whether the information sought here would significantly alter the quantum of proof in the defendant's favor.

With respect to the circuit law, I think a review of the opinions relied on in the *Michaud* case makes clear that the standard is different there. In the *Munez* --

THE COURT: Well, does that recent decision by the Fourth Circuit on the question of the transmission tower impact your argument on that point?

MS. GRATTON: I don't believe so, Your Honor. I don't have that opinion immediately available in front of me; however, I am aware that the en banc --

THE COURT: Well, that opinion came out at the same time as my opinion came out, so I didn't have the benefit of

it when I wrote my opinion.

MS. GRATTON: But in that case the Court did determine that in order to seek those orders, the orders at issue in those cases for the cell tower information, that the government was not required to obtain a warrant based on probable cause.

Unfortunately, I don't have the opinion immediately in front of me. I'd be happy to submit any additional briefing the Court would like on that question.

THE COURT: I'm familiar with it.

MS. GRATTON: But in the *Munez-Walkez* opinion out of the Ninth Circuit -- or, excuse me, *Hernandez-Meza*, both of which were cited by the Court in *Michaud* and appear to be the standard on which the Court made its materiality finding, describe materiality as a low threshold and said that anything that would allow a defendant to completely abandon a planned defense or take a different path is material. Well, when you compare that to the language in *Caro*, it says, "Evidence is material if its disclosure would enable him to significantly alter the quantum of proof in his favor."

So reading those two standards side by side, the government does think that there is a material difference there that would warrant a ruling that -- especially in light of the failure to show any issues of irregularity here, in light of the evidence that has been disclosed and, frankly,

the failure to even fully examine the evidence that is available to him, that at this point the defendant has not made a showing of materiality sufficient to order any further disclosure of information related to the delivery of the NIT.

Additionally, the government has offered for the Court's ex parte and in camera consideration a classified briefing related to the question of privilege. The general outlines of the issues raised in that filing were included in the sealed declaration attached as Exhibit 2 to the government's surreply and made available to the defendant.

And it's the government's position, even if the Court were to find that the defendant has made a threshold showing of materiality, that the information is nonetheless privileged. And the question of disclosure is not resolved simply by the finding of materiality in and of itself, because we don't get to law enforcement privilege until we've decided that the information is material and otherwise subject to disclosure under Rule 16.

So if we're there, there has to be some showing beyond that of a compelling need for the information that outweighs the public's interest in keeping it private and secret.

THE COURT: Well, the entire case is about the public's interest in being protected from child pornography, on the one hand, as against the right of privacy implied by

the Fourth Amendment, on the other.

MS. GRATTON: As the Court noted in its ruling on the first and third motions to suppress, that is the balance that must be struck here. And at least with respect to the suppression question, the Court found the balance struck in favor of the public's interest.

So the government would ask the Court to consider the information submitted for the ex parte and in camera review. Mr. Prabhu, my colleague, is here to address any further questions in that setting, if the Court has them.

And so, even if the defendant has shown materiality, he has not shown anything beyond that that would indicate a compelling need for the information sufficient to overcome the public's interest in keeping it secret, particularly in light of the fact that we are dealing here with speculative claims about what could have happened, what might have happened, without any facts showing that any of that did happen. The government provided extensive discovery. There are additional steps that the defendant can take.

Thank you, Your Honor.

THE COURT: Thank you.

MR. GRINDROD: I'll be quick, Your Honor, if I may.

THE COURT: You may.

MR. GRINDROD: Your Honor, just to address two points raised by the government, one, with respect to the

showing of materiality, the *Caro* case, the Fourth Circuit case that the government cites, says that, "Evidence is material as long as there's strong indication that it will play an important role in uncovering admissible evidence, aiding in witness preparation, corroborating testimony, or assisting impeachment or rebuttal."

Their argument against materiality is based solely on Agent Alfin's testimony in court and his declarations, but there's no way of either corroborating or impeaching that testimony if we don't have the evidence upon which it's based. That's what we're asking for.

Number two, Your Honor, I know the Court addressed various positions on materiality, and whoever has it may have some bias in this case. But I would note that on that question had we not filed this motion, the government's position in this litigation was that none of this information was material and they were not going to produce any of it. Now they're relying on this other information that they subsequently produced to say that, this other information that we want, that we asked for back in March, is not material.

Well, if their first position was none of it's material, and in their response to our motion they say, okay, you can have this part of it, and then in their surreply they say, okay, you can have this part, and now they're saying,

well, because we gave you this part, you don't need this other part you want -- we need it, Your Honor. We need the evidence. Mr. Matish has a constitutional right to putting on a defense, and we need the evidence to do so.

Thank you.

THE COURT: All right. When the Court prepared its opinion on the defendant's first and third motions to suppress, the Court ordered that it be filed under seal. At the time I was preparing that opinion the trial was imminent in the case, and I did not want the trial of the case to become a media event, which I thought might affect the Court's ability to give the defendant a fair trial.

Since then, the case has been certified as a complex case and the case has been postponed. The defendant didn't ask that it be placed under seal; the Court made that decision. I don't know whether the defendant believes that it should be continued under seal at this point in the proceeding or not.

MR. GRINDROD: Your Honor, that's something I've not really discussed in depth with my client. If it would please the Court, if I could have a day or until later this afternoon to notify the Court of our position on that --

THE COURT: I don't know. I mean, I -- you know, sometimes when cases involve a difficult or controversial issue, which this case certainly does, they change the case

to somebody against John Doe, or something like that, because somebody doesn't want their name forever associated with a case, regardless of the outcome, when it involves a sensitive topic like child pornography.

So I don't know what to tell you about that. All I can say is if the defendant wants the opinion under seal, I'll certainly consider that.

MR. GRINDROD: I appreciate it, Your Honor. I'll make a filing of some sort one way or the other, if it pleases the Court.

THE COURT: But I need for you to do that quite soon.

MR. GRINDROD: Yes, Your Honor, understood.

THE COURT: All right. Well, having initially placed its opinion under seal, and not having an answer as to whether the defendant wants it to remain so, I will not go into the Court's thinking at this time. I'll prepare a written opinion, which I would do anyway, but I'll hold off on publishing any opinion until I hear from the defendant on that issue.

Do you think you can let me know --

MR. GRINDROD: This afternoon, Your Honor.

THE COURT: Okay. All right.

Is there anything further from either side, then?

MS. GRATTON: No, Your Honor.

MR. GRINDROD: Nothing from the defense, Your Honor.
THE COURT: All right. Are there any remaining pretrial motions pending, other than this discovery motion?
MS. GRATTON: No, Your Honor.
THE COURT: All right. Well, I mean, some of the discovery has been handled by agreement between the parties, and the Court is really not privy to all that.
MR. GRINDROD: Correct, Your Honor.
MS. GRATTON: Yes, Your Honor.
THE COURT: So as far as I know, this is the only motion that the Court hasn't decided.
MR. GRINDROD: I think that's right, Your Honor.
MS. GRATTON: That's correct, Your Honor.
THE COURT: All right. Well, I'll wait to hear from you, then, Mr. Grindrod.
I don't think it's necessary, regardless of the Court's decision, to have an in camera hearing. I've been supplied with the government's brief that was marked "Secret," which I have reviewed, and I think that the materials that I reviewed in preparation for this hearing would enable the Court to make a decision on whether the privilege would apply if the Court finds the evidence material without the necessity of an in camera hearing.
(The hearing adjourned at 1:35 p.m.)

CERTIFICATION

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

/s

Heidi L. Jeffreys

June 16, 2016

Date