```
 1                  IN THE UNITED STATES DISTRICT COURT
                   FOR THE EASTERN DISTRICT OF VIRGINIA
 2                           Norfolk Division

 3  - - - - - - - - - - - - - - - - - - -
      UNITED STATES OF AMERICA,        )
 4                                      )
              Plaintiff,                )
 5                                      )        CRIMINAL CASE NO.
      v.                                )           2:16cr00036
 6                                      )
      GERALD ANDREW DARBY,              )
 7                                      )
              Defendant.                )
 8    ---------------------------       )
      UNITED STATES OF AMERICA,         )
 9                                      )
              Plaintiff,                )
10                                      )        CRIMINAL CASE NO.
      v.                                )           2:16cr00043
11                                      )
      HUNTER VAUGHAN EURE,              )
12                                      )
              Defendant.                )
13  - - - - - - - - - - - - - - - - - - -

14                      TRANSCRIPT OF PROCEEDINGS
                            Norfolk, Virginia
15                            July 5, 2016

16


17  BEFORE:    THE HONORABLE ROBERT G. DOUMAR,
               United States District Judge
18
    APPEARANCES:
19
               UNITED STATES ATTORNEY'S OFFICE
20             By:  Elizabeth M. Yusi
                    Leslie W. Fisher
21                  Assistant United States Attorneys
                    Counsel for the United States
22
               FEDERAL PUBLIC DEFENDER'S OFFICE
23             By:  Andrew W. Grindrod
                    Richard J. Colgan
24                  Rodolfo Cejas, II
                    Assistant Federal Public Defenders
25                  Counsel for the Defendants
```

```
 1                            I N D E X

 2
     ON BEHALF OF THE DEFENDANTS:     Direct   Cross   Red.   Rec.
 3
     C. Soghoian, Ph.D.                  5       64     --     --
 4
     (Recalled)                        148      153     --     --
 5

 6
     ON BEHALF OF THE GOVERNMENT:
 7
     D. Alfin                           96      102    136    142
 8

 9

10

11

12
                           E X H I B I T S
13
     No.                                                    Page
14
     Government's Exhibit 1                                   71
15
     Government's Exhibit 2                                   80
16

17
     Defendant's Exhibit 1                                    94
18

19

20

21

22

23

24

25
```

1   (The proceedings commenced at 2:30 p.m., as

2   follows:)

3   THE CLERK: Criminal Case No. 2:16cr36, United

4   States of America v. Gerald Andrew Darby.

5   Ms. Fisher, Ms. Yusi, are you ready to proceed on

6   behalf of the United States?

7   MS. YUSI: We are.

8   Good afternoon, Your Honor.

9   THE CLERK: Mr. Cejas, are you ready to proceed on

10   behalf of the defendant?

11   MR. CEJAS: Yes, we are.

12   THE CLERK: And in Case No. 2:16cr43, the United

13   States v. Hunter Vaughan Eure, Ms. Yusi, Ms. Fisher, are you

14   ready to proceed?

15   MS. YUSI: We are, Your Honor.

16   THE CLERK: And Mr. Grindrod and Mr. Colgan, are you

17   ready to proceed on behalf of the defendant?

18   MR. GRINDROD: We are.

19   Good afternoon, Your Honor.

20   THE COURT: I would like to take up the motion to

21   suppress by Mr. Eure first, which we haven't ruled upon, and

22   then we will deal with the motions to compel jointly so that

23   we just don't reiterate everything and we won't have two.

24   So let's take up Mr. Eure's motion to suppress at

25   this time. And I assume, Mr. Grindrod, you're arguing that.

 1   MR. GRINDROD: I am, Your Honor, and we also have

 2   evidence, if we could, Your Honor.

 3   THE COURT: All right. I'll be glad to hear from

 4   you. It's your motion.

 5   MS. YUSI: May I have a moment, Your Honor?

 6   THE COURT: Sure.

 7   (There was a pause in the proceedings.)

 8   THE COURT: All right. Go ahead.

 9   MR. GRINDROD: Your Honor, the defense calls

10   Dr. Christopher Soghoian to the stand.

11   (The clerk administered the oath.)

12   MR. GRINDROD: And, Your Honor, Dr. Soghoian is

13   going to be testifying as to matters that relate both to

14   suppression and the motions to compel. I can separate them

15   and recall him later, or I can ask all the questions at once,

16   Your Honor.

17   THE COURT: Well, since we're having a joint

18   hearing, my suggestion is he's going to testify in both, and

19   maybe that would save us some time, assuming counsel for

20   Mr. Darby would agree.

21   MR. CEJAS: Yes, sir, that's fine.

22   THE COURT: Thank you, Mr. Cejas.

23   MR. GRINDROD: May I inquire, Your Honor?

24   THE COURT: Yes, go ahead.

25   CHRISTOPHER SOGHOIAN, Ph.D., called as a witness,

1 having been first duly sworn, testified as follows:

2 DIRECT EXAMINATION

3 BY MR. GRINDROD:

4 Q. Good afternoon, sir. Could you please introduce yourself

5 to the Court.

6 A. My name is Christopher Soghoian.

7 Q. And why are you here today, sir?

8 A. I volunteered in my personal capacity as an expert so

9 that the defense and so that the Court can have a better

10 understanding of the technology used by the FBI in this case.

11 Q. Okay. I want to talk to you about a little bit of

12 background, about your experience and qualifications. Could

13 you tell us a little bit about your educational background?

14 A. Sure. I have a Bachelor's degree in computer science

15 from James Madison University, I have a Master's degree in

16 security informatics from the Johns Hopkins University, and I

17 have a Ph.D. in informatics from Indiana University.

18 Q. Can you tell us a little bit about your experience

19 working in these fields?

20 A. Sure. So in my job at the ACLU and before that at the

21 Federal Trade Commission I am a computer scientist who

22 explains technology to lawyers.

23 My Ph.D. was focused in the analysis of surveillance

24 techniques used by the U.S. Government, and specifically I

25 help lawyers understand how the government engages in high

1   tech surveillance. So at the ACLU, where I'm employed, I

2   work with the lawyers who litigate Fourth Amendment cases,

3   and I make sure that they understand the technology and that

4   they are accurately describing it in the cases in which

5   they're engaged.

6   Q.   And what is your position at the ACLU?

7   A.   I'm employed as the ACLU's principal technologist in our

8   Speech Privacy and Technology Project.

9   Q.   Do you currently hold any other position?

10 A.   I'm also a visiting fellow at the Information Society

11 Project at Yale Law School.

12 Q.   And have you received any awards or honors in your field?

13 A.   I've received a couple of awards. Politico magazine last

14 year named me one of the top 50 people affecting policy in

15 the United States. That's the one I can remember off the top

16 of my head.

17 Q.   That's fine. Have any courts cited your work?

18 A.   My academic research on surveillance has been cited by a

19 few federal courts, including the Ninth Circuit Court of

20 Appeals, and by the State Supreme Courts of Massachusetts and

21 New Jersey.

22   THE COURT: Where was this academic research? You

23 just said your academic research.

24   THE WITNESS: Yeah. I have law review articles that

25 have been published in the Harvard Journal of Law and

1 Technology, the Berkley Journal of Law and Technology, and

2 the Yale Journal of Law and Technology, and so that research

3 has been cited by those courts.

4 BY MR. GRINDROD:

5 Q. And has any of your work focused specifically on remote

6 technology or malware?

7 A. I've been researching NITs, the network investigative

8 techniques, for about five years, and in the course of that

9 research I have learned quite a bit about the technology,

10 I've interviewed people who have worked in the teams at the

11 FBI that deliver this technology, and I've analyzed some of

12 the code that the FBI has used.

13 Q. And have you done -- we've talked a lot about the

14 training you've received. Have you given any training or

15 spoken on these topics?

16 A. Sure. So I've been invited to several training events

17 organized by the Federal Judicial Center, so I've given

18 training to judges, both District Court Judges, Magistrate,

19 and even Circuit Court Appellate Judges, about surveillance

20 technology, including the use of NITs.

21 Q. Have you offered testimony before any legislative bodies

22 or rule-making committees about these topics?

23 A. Yeah. I've testified before, I think, three different

24 state legislative bodies in the United States, the European

25 Parliament, and I also testified before the rules committee

1   that put out the changes to Rule 41 regarding the use of

2   these technologies.

3   Q. Okay. And now I want to talk to you specifically about

4   your preparation for your testimony in this case.

5   First of all, do you have any background knowledge on

6   NITs or network investigative techniques?

7   A. So, as I said, I've been researching NITs for about five

8   years. I've testified in two cases, two prior cases where

9   NITs have been used, as a volunteer, an unpaid volunteer, for

10 the defense in those cases. I've reviewed numerous case

11 filings. I've reviewed transcripts from Special Agent Alfin

12 and others.

13   And then, under protective order in various cases,

14 I've looked at some of the code and some of the two-way

15 network recordings as well.

16 Q. Okay. Have you looked at the code and the PCAP data that

17 was produced in Mr. Eure's case?

18 A. I have.

19 Q. You said you're here in your personal capacity. Is that

20 right?

21 A. Yes.

22 Q. Are you being paid for your services in this case by the

23 defense?

24 A. My flight was paid for, and I think my taxi fees will be

25 reimbursed, but I'm not receiving any kind of honorarium or

1   consulting fee, no.

2   Q. Okay. So why is it that you volunteer in cases like

3   this?

4   MS. YUSI: I object, Your Honor. What's the

5   relevance of this?

6   THE COURT: Objection sustained.

7   BY MR. GRINDROD:

8   Q. I want to talk to you about --

9   A. I'm sorry. Can I get a glass of water, too? Is that

10 possible?

11   MR. GRINDROD: Yes.

12   (There was a pause in the proceedings.)

13 BY MR. GRINDROD:

14 Q. Are you familiar -- I want to talk to you about a couple

15 issues having to do with suppression. So, first, are you

16 familiar with the government's argument that the NIT that was

17 deployed in this case --

18   THE COURT: Stop. You're getting into the case

19 itself so, consequently, are you finished with the voir dire

20 of this witness's qualifications?

21   MR. GRINDROD: Yes, Your Honor.

22   THE COURT: Ms. Yusi, do you have any questions on

23 voir dire?

24   MS. YUSI: I don't, Your Honor, but I also don't

25 know what he's being offered for as an expert in.

 1   THE COURT: Well, I'm sure he'll tell us.

 2   MS. YUSI: Okay.

 3   THE COURT: Go ahead, Mr. Grindrod.

 4   MR. GRINDROD: Thank you, Judge.

 5   BY MR. GRINDROD:

 6   Q. Are you familiar with the argument that's been raised by

 7   the government in this case and related cases that the NIT

 8   that was deployed in this case worked like a tracking device?

 9   A. I am familiar with that theory.

10   Q. And just so we're on the same page, that argument goes,

11   basically, that a Playpen user entered the government server

12   hosting Playpen, which --

13   MS. YUSI: Objection, Your Honor. He's testifying.

14   If he wants to ask a direct question...

15   THE COURT: Objection sustained.

16   BY MR. GRINDROD:

17   Q. Can you tell me what your understanding of the

18   government's argument is with respect to this tracking

19   device?

20   THE COURT: It's not the government's argument, it's

21   what his understanding of what is utilized in this case is.

22   Don't let's talk about somebody else's argument.

23   He's not an expert on the argument, okay? He's an

24   expert on the use of the Internet. He can also describe all

25   of his uses. He can tell me what a NIT is, but he's not

1   going to tell me whether the argument of the government is

2   appropriate or inappropriate in any way. He can discuss all

3   he wants about any factual matter or his opinions, but not

4   his opinions of somebody else's case.

5   Do we understand one another, sir?

6   MR. GRINDROD: Yes, Your Honor.

7   THE COURT: Okay.

8   BY MR. GRINDROD:

9   Q.   Can you tell me from a technological perspective where

10   the NIT is installed, the location, the physical location?

11   A.   So the computers that were visiting the Playpen Web site

12   ultimately had to contact the government server, which was

13   located somewhere in Northern Virginia. Although the code,

14   the computer instructions for the NIT, was hosted on the

15   government's computer, it didn't activate. It didn't do

16   anything until it was transmitted all the way over the

17   Internet to the receiving parties, to the computers that were

18   visiting the Web site, and then ultimately ran on those

19   individual computers.

20   THE COURT: You lost me, so let's go back.

21   THE WITNESS: Let's try again. Okay.

22   So there were a number of people who visited the

23   Playpen Web site. They connected to the Playpen Web site

24   using this technology called Tor, but ultimately there was a

25   Web browser, like Firefox or Internet Explorer or Chrome, and

1 then they used their Web browser to visit a Web site.

2   The NIT, the network investigative technique, was

3 delivered to the computers of the people who were visiting

4 this Web site, and the network investigative technique --

5   THE COURT: Well, what you have to do is to say what

6 visited the network site, not "the NIT visited."

7   "The NIT visited" is too broad a concept.

8 That's investigative techniques. So what we want to deal

9 with are the specifics, and that's what I've got to hear.

10 Otherwise, you just become another attorney for the

11 defendant. Don't become the attorney, just become the

12 expert, okay?

13   THE WITNESS: Yes, Your Honor.

14   And, to be clear, I'm not an attorney. I didn't go

15 to law school.

16   THE COURT: Well, by the time you finished

17 explaining your background, you probably know more than most

18 attorneys who are dealing with this subject.

19   THE WITNESS: I appreciate that, sir.

20   THE COURT: So let's get on with what we're doing

21 here.

22   First, one thing I want to find out about

23 qualifications -- I might as well do it now that I've

24 interrupted you -- is are you paid a salary by the ACLU?

25   THE WITNESS: I am paid a salary, sir, but I'm

1   taking a vacation day to come here.

2   THE COURT: You're taking a vacation?

3   THE WITNESS: A one-day vacation.

4   THE COURT: Do they give you vacation days?

5   THE WITNESS: I receive vacation days at the ACLU.

6   Not as many as I would like.

7   THE COURT: So what I'm getting at is you're not

8   losing any money, as such.

9   THE WITNESS: No, I'm not.

10   THE COURT: And when you say you're an unpaid

11   volunteer, you are a volunteer here, but I assume it's with

12   the understanding of the ACLU.

13   THE WITNESS: I have to ask my boss for permission

14   to take time off, yes.

15   THE COURT: I figured that. So I just want to know

16   where we are and what we are dealing with. So, consequently,

17   you can go on from there, but let's stick to the facts and

18   your expertise, okay?

19   MR. GRINDROD: Thank you, Your Honor.

20   THE WITNESS: Sir, if I might add one more thing, I

21   just want to clarify.

22   I asked to come here from my -- I asked for

23   permission from my employer, as opposed to being told by my

24   employer, "Hey, Chris, take a day off and go down to

25   Norfolk."

1   THE COURT: Oh, I understand that.

2   BY MR. GRINDROD:

3   Q. Okay, Dr. Soghoian. So I think you were starting to

4   explain kind of the technology -- how the NIT works from a

5   technological standpoint. So if you could tell us where --

6   first of all, what is -- Judge Doumar just asked this.

7   So what is the NIT? When we're talking about the NIT

8   and we talk about code associated with it, can you just tell

9   us what that is?

10   A. The NIT is a specially made computer program that is

11   designed to surreptitiously collect information from one or

12   more person's computers, collect that information, and

13   transmit it back to the government.

14   Q. Okay. So even kind of more specifically than that, when

15   we talk about the NIT being computer code, what is that?

16   What is computer code?

17   A. So if you think of the blueprints for a building versus

18   the building itself, human beings write code, and computer

19   scientists who know how to write computer programs, they

20   create code by writing it in a special language. But it's

21   still human readable, readable by humans who understand

22   computers, and then the computer turns it into a special

23   language that is easier for the computer to understand. So

24   that's called computer code.

25   Q. Okay.

1   A. And, essentially, they're a series of instructions that

2   tell the computer, do this, do that, do this other thing.

3   Q. And computer code, is that something that only exists in

4   the government surveillance context, or does computer code

5   exist --

6   A. No, every single electronic device that we have in our

7   lives, from a cell phone to an ATM machine to an airplane,

8   has computer code in it now.

9   Q. So the question I asked you a little while ago was trying

10 to understand where the computer code that we're talking

11 about in this case, the NIT, where that actually was

12 deployed, where it worked. So can you explain, just from a

13 technological perspective, focusing on the facts, where that

14 happened?

15 A. Sure. The computer code, the NIT code in this case,

16 would have been downloaded from a server run by the FBI in

17 Northern Virginia, downloaded to the computers of the

18 individual people visiting the Playpen site, including the

19 alleged defendants in this case. But it would not have run,

20 the code would not have done anything, until it reached their

21 computers and ran on their computers.

22   You could think of the code as being inert. It

23 didn't have the power to do anything until it ran on the

24 computers of the individual defendants.

25 Q. And was the -- until the code was installed on our

1 client's computer, would there have been -- did it serve any

2 functional purpose for anyone who would have been using the

3 code?

4 A. The code would never have run on anyone's computers but

5 the defendant's computer, you know, unless an FBI agent ran

6 it in the lab to test it out. But when it was sitting on the

7 government's Web server, its Web site, waiting to be

8 downloaded it would be sitting dormant. It wasn't doing

9 anything. It wasn't hurting anyone or helping anyone. It

10 was just sitting there like an unopened piece of mail, and

11 someone had to go and get it, bring it back, and it was only

12 then, once it was executed on the defendant's computer, that

13 it would come to life and that it would have the resources to

14 then run. And with those resources with a computer that had

15 power and had the ability to think, the processing

16 capability, then the NIT could come to life and perform the

17 instructions that it had been programmed to do; in this case,

18 to collect various forms of information from the computer

19 that it was operating on and then to call home to the

20 government server with those bits of information.

21 Q. In any technological sense, did the user of an activating

22 computer visit the FBI's server?

23 A. The individual users of the Playpen site certainly

24 communicated with the government's server. They requested

25 Web pages, and the Web pages were then returned to those

1   individuals. Those individuals never left their homes. They

2   didn't get in their car and drive across country or up --

3   THE COURT: So the code had nothing to do, then,

4   with the requested Web pages of the --

5   THE WITNESS: The Web pages were viewed by the

6   individual users --

7   THE COURT: I'm asking once it was sent to the

8   government -- to Playpen, we'll call it, and you're familiar

9   with it. The code had nothing to do with that.

10   THE WITNESS: The code --

11   THE COURT: The code is merely an investigatory

12   matter, correct?

13   THE WITNESS: The NIT code was delivered to the

14   visitors of the site at the same time as they were visiting

15   the Web page.

16   THE COURT: I understand, but the site itself would

17   know what was requested of it, correct?

18   THE WITNESS: When you say "the site," I mean --

19   THE COURT: Playpen.

20   THE WITNESS: I understand Playpen, but Playpen was

21   a Web site, it wasn't a human, so when you say did the site

22   know do you mean the people operating the Web site, did they

23   know? Because they were FBI agents, they definitely knew

24   what was being delivered.

25   THE COURT: Once the Web site gets something, does

1   the Web site know it got it?

2   THE WITNESS: The --

3   THE COURT: Does it record?

4   THE WITNESS: I think I know what you're asking.

5   When the NIT called home it did not call home to the

6   Playpen site. The NIT was delivered to people who were

7   visiting Playpen; that when the NIT called home it called

8   home to a different computer run by the FBI.

9   THE COURT: All I'm asking you is Playpen. It

10 receives something, correct?

11   THE WITNESS: The -- when the user visits the

12 Playpen site, they request a Web page. They get that Web

13 page back, and that response would have included -- I'm

14 trying to figure out how to explain this in terms that are

15 easy to --

16   THE COURT: Playpen responds to whatever the request

17 is, and all I'm saying is there's a record of that response,

18 correct?

19   THE WITNESS: When you say -- you mean a permanent

20 record?

21   THE COURT: I don't know if it's permanent or

22 anything. I assume Playpen has some knowledge of what it

23 sends.

24   THE WITNESS: That would really depend on how the

25 FBI configured the Playpen site.

1   THE COURT: I'm not worried about the FBI, I'm

2   worried about Playpen, the site itself.

3   Once the FBI runs it, it's just running a site,

4   correct?

5   THE WITNESS: Again, that really depends on how the

6   FBI is running the site. If I can use an analogy, Your

7   Honor, the PACER Web site that this court runs that people

8   can download documents from, there may be records that are

9   kept of every document I download from PACER; there may not

10   be. It really depends on how the administrators of this

11   courthouse configure the Web site to operate.

12   I don't know whether the FBI, when they were

13   operating the Playpen site -- whether they recorded every

14   single thing that the Web site sent or nothing.

15   THE COURT: So the FBI has the site, correct?

16   THE WITNESS: The FBI was running the Playpen site,

17   yes, sir.

18   THE COURT: And they don't know what's happening on

19   the site. Is that your testimony?

20   THE WITNESS: No, Your Honor.

21   THE COURT: Oh, so they know what's happening on the

22   site.

23   THE WITNESS: Your Honor, I'm saying I don't know

24   what the FBI knew because I don't know how the FBI configured

25   Playpen. And the Playpen site is no longer operational, so I

1   cannot go and check.

2   THE COURT: So you didn't look into that information

3   at all when you were investigating this matter, correct?

4   THE WITNESS: It would be a crime for me to visit

5   the Playpen site, Your Honor, when it was up and running.

6   THE COURT: Excuse me. You can help me a lot -- if

7   you answer questions, you can answer "yes" or "no" and make

8   any explanation you desire. Otherwise, I may have trouble

9   understanding your answers.

10   Now, let's go back over that. Let's go back. You

11   say you don't know what the FBI knew when it was

12   administering the site. Is that correct?

13   THE WITNESS: That is correct, sir.

14   THE COURT: So -- okay. Go ahead.

15   MR. GRINDROD: Thank you, Your Honor.

16   BY MR. GRINDROD:

17   Q. So this NIT, as the government has stated -- one of

18   the -- is it your understanding that one of the reasons the

19   government ran the NIT was to find out geographically where

20   the user's computer was located?

21   THE COURT: He hasn't testified to that yet, and so

22   be careful about leading the witness. I will allow it,

23   because we pretty well know that he's been informed of a

24   great many things, but don't lead witnesses, okay?

25   But that question I'm going to allow. I'm just

1   warning you, don't do it again.

2   MR. GRINDROD: I'm warned. Thank you, Your Honor.

3   THE WITNESS: So the Tor software that everyone was

4   using to access the Playpen site, that protects -- more than

5   anything else, that is designed to protect the IP address of

6   each person visiting the site.

7   THE COURT: So you're familiar with that software.

8   THE WITNESS: I'm familiar with Tor, yes, sir.

9   THE COURT: I understand you're familiar with Tor.

10 Are you familiar with the software that Tor employs?

11   THE WITNESS: Yes, Your Honor, I'm familiar with the

12 Tor browser, which is the software I think that we're

13 discussing.

14   THE COURT: So you've looked at that software

15 before.

16   THE WITNESS: I've used that software. The tool was

17 created by the government ten years ago, and it's --

18   THE COURT: It's created by the Navy. Were you a

19 part of that creation?

20   THE WITNESS: No, sir. It was created with by the

21 U.S. Naval Research Lab originally and then was subsequently

22 spun out into a nonprofit, but I've never been a developer of

23 Tor or employed by the Tor organization.

24   But some of the developers taught classes at my

25 Ph.D. university, and I know some of the developers who work

1   on it.

2   THE COURT: My curiosity abounds. And what were

3   their names?

4   THE WITNESS: Sorry. What was the question, sir?

5   THE COURT: You said you knew the developers because

6   they taught you at the university. What were their names?

7   THE WITNESS: So Paul Siverson, who is employed by

8   the U.S. Naval Research Lab still to this day, he was a

9   visiting professor for a semester at my university.

10   THE COURT: And so he taught you a course?

11   THE WITNESS: Yeah, I think he gave one guest

12   lecture in --

13   THE COURT: One lecture?

14   THE WITNESS: One lecture.

15   BY MR. GRINDROD:

16   Q. Dr. Soghoian, let me ask you about the government's --

17   so, again, going back to my original question, before the

18   government deployed the NIT did the government have any

19   understanding of where geographically an activating computer

20   was located?

21   A. It would have been extremely difficult, if not

22   impossible, because the Tor browser and the Tor network

23   software are designed, first and foremost, to shield that

24   information from everyone who might wish to discover it.

25   Q. And was --

1   THE COURT: Doesn't the person who is trying to get

2   the information have to give the computer that it sends to

3   information where to send the material?

4   THE WITNESS: So that's why Tor is such an

5   interesting tool. When you use Tor to browse the Internet --

6   let's say you're visiting CNN, you look for an article on the

7   CNN Web site. CNN doesn't actually know where they're

8   sending it, so the data gets bounced around through a bunch

9   of servers, and so no one --

10   THE COURT: How do they get the information, then?

11   THE WITNESS: If you --

12   THE COURT: It's not being sent back.

13   THE WITNESS: Instead of the data being sent

14   directly from CNN to your personal computer, it gets sent

15   through a couple intermediaries along the way, and they --

16   THE COURT: I know about coming to the Playpen. Now

17   something leaves the Playpen, I assume.

18   THE WITNESS: Just as the connection from the user

19   to the Web site goes through the intermediaries, the

20   responses go back through the same intermediaries. And the

21   intermediaries are servers run by volunteers around the

22   world.

23   BY MR. GRINDROD:

24   Q. So before the NIT is deployed does the government have

25   any idea where in the world the activating computer is

1   located?

2   A. No.

3   Q. Okay. So I want you to imagine for me, then, a warrant

4   that authorized the government to deploy this NIT but only

5   against computers that were located in the Eastern District

6   of Virginia. From a technological perspective, how would

7   that warrant be executed?

8   A. There would be no way to limit the execution of a NIT to

9   only computers located in the Eastern District of Virginia,

10 because until the government hacks into the computers of the

11 targets they won't know where they are -- I'm sorry. The

12 government will not know where the defendants' computers are.

13 Q. Understood. I want to shift gears now for a moment and

14 talk to you about some issues related to the pending motion

15 to compel.

16   So at various points in the briefing the parties have

17 referred to the NIT as having different components. Are you

18 familiar with that terminology?

19 A. Yes, sir.

20 Q. Okay. In Mr. Eure's case, at least, the government has

21 produced the two components of that, right?

22 A. Yes, the --

23 Q. Can you tell us what components?

24 A. I've reviewed and analyzed the NIT --

25   THE COURT: First tell us what two components they

1 are, then you tell us what you analyzed.

2   THE WITNESS: Yes, Your Honor.

3   The two components are the NIT, the network

4 investigative technique, and what's known as a PCAP, P-C-A-P,

5 file. This is what the government, I believe, has referred

6 to as a two-way network recording.

7 BY MR. GRINDROD:

8 Q. And two other components that exist but have not been

9 produced, is one of those the exploit?

10   MS. YUSI: Your Honor, I object.

11   THE COURT: You know, I asked you not to lead the

12 witness.

13   MR. GRINDROD: I'll rephrase, Your Honor.

14   THE COURT: I'm not going to do it anymore.

15   MR. GRINDROD: I'll rephrase, Your Honor.

16   THE COURT: Next time you'll know what happens, but

17 don't do it again. And I asked you not to do it the last

18 time.

19   MR. GRINDROD: I understand, Your Honor.

20   THE COURT: And I don't expect you to do those

21 things if I tell you don't do it, okay?

22   He's perfectly capable of discussing it. He's been

23 testifying. He's a volunteer. I'm not worried about him not

24 knowing what's going on, but I am worried about leading the

25 witness.

1   MR. GRINDROD: I understand, Your Honor.

2 BY MR. GRINDROD:

3 Q. You mentioned two parts of the four components. Can you

4 tell us what the other two are?

5 A. The other significant components that are missing that I

6 haven't reviewed and that haven't been disclosed are the

7 exploit and the code that generates the unique serial numbers

8 for the individual NIT deliveries.

9 Q. Okay. I want to talk about --

10   THE COURT: Slow down. One is called the exploit.

11   THE WITNESS: An exploit, yes, sir.

12   THE COURT: What is the other one?

13   THE WITNESS: The second one is a special code that

14 would have run on the government's server that generated

15 unique serial numbers each time the NIT was deployed.

16 BY MR. GRINDROD:

17 Q. I want to have you just --

18   THE COURT: And that is not the exploit?

19   THE WITNESS: No, sir. And if you would like, I can

20 go through each component and say what they do.

21   THE COURT: I'm just trying to make sure where I'm

22 going, because you're going to be discussing these terms. I

23 want to be able to understand them.

24   Okay. Go ahead.

25 BY MR. GRINDROD:

1   Q. I do want to go through each of these components with you

2   just to get an understanding of what they are, and then we'll

3   talk later about why they may be important for various --

4   THE COURT: How much time do you expect for this

5   witness?

6   MR. GRINDROD: It's going slower than I expected,

7   Your Honor, but another half hour, at most.

8   THE COURT: All right. You have another half hour,

9   period.

10   MR. GRINDROD: Thank you, Your Honor.

11   THE COURT: Because, otherwise, we won't get

12 finished today.

13   MR. GRINDROD: I understand, Your Honor.

14 BY MR. GRINDROD:

15 Q. You mentioned the NIT computer code. Can you tell us

16 what that is, briefly?

17 A. Yes. The NIT code has two pieces of functionality. The

18 first is that it collects specific information from the

19 computers on which it runs. That might be the serial number

20 of the Wi-Fi card, information about the operating system

21 that's running on the computer.

22   Once it has compiled that information, the second

23 piece takes over, and that transmits that collected

24 information back to an FBI-controlled server.

25 Q. The PCAP data, can you tell us what that is?

1   A.   The PCAP data is a recording created at a government

2   facility that purports to show what the government received

3   from the individual NIT users.

4   Q.   The exploit, what is that?

5   A.   As I said before, the Web browser that people are using,

6   that is designed to visit Web pages, and the Tor browser is a

7   special Web browser that is designed to be more secure than

8   the average Web browser.

9   The piece of information that it is designed to

10   protect, first and foremost, over everything else, is the IP

11   address of the user. The Tor browser is designed so that if

12   a Web site asks, "What is your IP address?" it will say,

13   "No," and it is designed to resist any creative attempts to

14   try and learn the user's IP address.

15   For the NIT to be able to successfully run on the

16   computer of the targets, the first thing the government needs

17   to be able to do is to somehow bypass these strong security

18   features built into the Tor browser. And, so, if you think

19   of the Tor browser as a house guarded by trained guard dogs,

20   the exploit is a piece of meat that's been laced with

21   sleeping pills so the guard dogs fall asleep and let the

22   government go inside the house. So the exploit is the code

23   that bypasses or circumvents the security settings and

24   protections in the Tor browser.

25   Q.   And then the final piece is the unique ID generator --

1   THE COURT: The exploit is the thing that tells them

2 what computer is coming in on that particular information?

3   THE WITNESS: No, Your Honor, the NIT is the code

4 that identifies the computer and sends that information back

5 to the FBI server.

6   The exploit is the code that disables the security

7 protections of the Tor browser so that the NIT can then be

8 installed and execute.

9 BY MR. GRINDROD:

10 Q. So if the question is what let you in --

11   THE COURT: Hold on a minute.

12 BY MR. GRINDROD:

13 Q. What's the -- what let you in or what allowed the

14 government --

15   THE COURT: Stop a minute so I'll understand where

16 we're going.

17   First you find the name of the computer; that is,

18 the individual computer?

19   THE WITNESS: No, Your Honor. That's actually one

20 of the later stages.

21   The first thing the government has to do is get the

22 defendants' computers into a state where they will allow the

23 NIT to run. Normally, the Tor browser software will refuse

24 to run something like the NIT, because first and foremost

25 it's designed to protect that information from outside

1   parties who might wish to learn it.

2   So the exploit has to disable the built-in security

3   features that are contained within the Tor browser, and it

4   does that through the use of what is called a security

5   vulnerability; that is, a design mistake in the software, in

6   the Tor browser software.

7   The Tor browser, like all pieces of software, is

8   made by humans --

9   THE COURT: So the exploit just destroys, in

10   essence, any security; that's it.

11   THE WITNESS: That's a good way of thinking of it,

12   sir, yes, sir.

13   THE COURT: All right.

14   BY MR. GRINDROD:

15   Q. Okay. And then the last component of the four is the

16   unique ID generator. Can you tell us briefly what that is?

17   A. Yes. The purpose of the ID generator -- when the

18   defendants or the targets visit the Playpen site and receive

19   the NIT and the exploit, they are given a unique number like

20   a serial number.

21   When the computers that are running the NIT call

22   home, in addition to transmitting back their serial numbers

23   and other information, they transmit back that number that

24   the government has given them. In essence, it allows the

25   government to associate a particular user on the Playpen site

1 with a particular successful operation of the NIT and, as a

2 result, the IP address that the government learns through the

3 NIT operation.

4 Q. Okay.

5 A. And it's through the unique numbers that they're able to

6 say, defendant X was this user name on this Web site, and

7 they were logged in for this many days, and they viewed these

8 posts. That gives them the ability to identify individual

9 users and their history on the sites.

10 Q. Understood. So let's focus first on the exploit.

11   Can you tell the Court why it's important from a

12 technological perspective to review the exploit? What would

13 that tell you?

14 A. The exploit is important for a few reasons. The NIT

15 collected a bunch of information from the computer, and

16 without knowing -- without experts being able to look at the

17 exploit, it's not possible to say which condition or state

18 the computer was in before it collected the NIT.

19   Let me use an analogy. If the government is

20 analyzing DNA in a lab, you want to know that the petri

21 dishes that they were using, the equipment in the lab, is

22 clean. You want to know that it's sterile before they test a

23 particular defendant's genetic sample.

24   If we cannot see the exploit, we do not know the

25 state in which the computer was in before it ran the NIT,

1 which calls into question the reliability, the forensic

2 reliability, of the evidence that the NIT then collected. So

3 that's the first reason.

4   THE COURT: So looking at any computer, you have to

5 know what it was before anything was done to the computer.

6 Is that correct?

7   THE WITNESS: It would certainly be helpful. If you

8 want --

9   THE COURT: I didn't ask you about "helpful."

10 Everything is helpful.

11   The question in my mind is if I were looking at a

12 computer, any computer -- let's forget this case. We're

13 talking about your expertise. If I were looking at a

14 computer and wanting to know what it's putting out, I'd have

15 to know in advance what it had on it before?

16   THE WITNESS: That is true. You would want to

17 know --

18   THE COURT: So nobody should ever be able to testify

19 what was on a computer, correct?

20   THE WITNESS: The --

21   THE COURT: They can't testify because they couldn't

22 possibly have known what was on it before, even if they

23 looked at the computer, correct?

24   THE WITNESS: There are many things that a computer

25 can do, but the --

1   THE COURT: I understand there are many things a

2   computer can do, and I can walk and run and talk and count to

3   ten, but that doesn't mean that I can't ask questions

4   concerning what's happening.

5   What I'm trying to find out is -- the statement

6   you're making is that unless I know what was there before I

7   cannot tell you what's there after.

8   THE WITNESS: If I could try and explain --

9   THE COURT: So anything I see is not real, because

10   it could have been different.

11   THE WITNESS: The --

12   THE COURT: I couldn't say that Mr. Grindrod is

13   there unless I knew he wasn't there yesterday, correct?

14   THE WITNESS: The exploit forces the computer to do

15   things that it would never normally do, and it puts -- it

16   stresses the computer or the software running on the

17   computer --

18   THE COURT: I know what the exploit does. This is

19   not the first case, by the way, and we've heard these terms

20   consistently.

21   And what I want to do is to make sure I understand

22   what you're saying in relation to the determination of how

23   the FBI learned of whose computer was calling their Playpen

24   site. And you're saying that the first way they learned is

25   by having the NIT, having exploit, that would allow them to

1   find the name of the individual calling, correct?

2   THE WITNESS: It's not the name of the individual --

3   THE COURT: Well, the name of the computer.

4   THE WITNESS: The name of the person logged in to

5   the computer, the unique serial number associated with their

6   Wi-Fi card, and some other information from the computer.

7   THE COURT: So all of this is generated towards

8   finding out that particular computer, correct?

9   THE WITNESS: You're asking me if that's why the

10 information is collected by the NIT?

11   THE COURT: Yes.

12   THE WITNESS: I believe that is why the FBI collects

13 information from those computers, yes, Your Honor.

14   THE COURT: All right.

15 BY MR. GRINDROD:

16 Q. So I think you mentioned --

17   THE COURT: I'll give you five minutes more by

18 virtue of the fact that I've interrupted you.

19   MR. GRINDROD: Thank you, Your Honor.

20 BY MR. GRINDROD:

21 Q. So you mentioned one of the reasons why it's important to

22 view the exploit, but I think you said there were other

23 reasons.

24 A. There's another significant reason that you would want

25 it. If you think of the computer as a house, you have a

1 front door, you have a lock on the door. As I said, the

2 exploit takes advantage of a security flaw in the software

3 that was there that most people may not have known about

4 ahead of time. So think of it as a design flaw in the lock

5 on your front door. So the government knows that there's a

6 flaw in your lock so they send a Special Agent who is skilled

7 in the art to stand there and pick the lock, and that gains

8 them access to your house, and then they can execute the

9 search inside the house.

10   Now, you could pick the lock, if you're skilled at

11 lock-picking, and leave no trace, and when you close the door

12 and you're done with the search the lock is in perfect

13 working order. But it's possible if you make a mistake you

14 could still gain access to the house, but you could break the

15 lock in the process, and then the lock may not work in the

16 future and other people could go inside that house after.

17   One of the reasons why it would be a really good

18 idea for the defense to be able to look at the exploit is to

19 see if the exploit leaves the computer in as secure a state

20 as the government found it or if it leaves the computer in a

21 more vulnerable state, where other parties might be able to

22 log in to the computer, download their own software to the

23 computer, download other content or contraband to that

24 computer.

25   And this is not a hypothetical concern. Tools

1 similar to NITs used by other governments have been analyzed

2 by experts, and --

3   THE COURT: Stop telling me unless you give me --

4 you know, the world is full of explanations, so we've got to

5 deal with specifics. Who did what to whom at what time?

6   THE WITNESS: Okay. So a specific example:

7   A tool like the NIT, used by the German police, was

8 analyzed a couple years ago by German security experts and

9 discovered to have security flaws in it that left the targets

10 of the authorized law enforcement investigations -- left

11 those computers vulnerable to compromise and search by

12 unauthorized third parties.

13   It is very difficult to design secure software, and

14 it's quite possible that the exploit may have flaws in it

15 that we don't know about, but if it left the computer in a

16 less secure state it's possible that other parties might have

17 been able to gain access to that computer at a later date.

18   THE COURT: So why would another party want to gain

19 access?

20   THE WITNESS: Your Honor, there are --

21   THE COURT: I didn't ask -- is there any evidence

22 that some other party tried to gain access? Did you hear of

23 any?

24   THE WITNESS: So criminals break into computers

25 every day.

1   THE COURT: I know that, but they generally break

2   into computers because they want to find out something,

3   correct?

4   THE WITNESS: No. There are many reasons why

5   criminals do it.

6   One frequent reason is not to steal information from

7   a computer but to use that computer as a staging point to

8   download and distribute other stolen information.

9   THE COURT: To break into that, wouldn't they have

10   to be able to know what it is they're breaking into?

11   THE WITNESS: No, Your Honor, there are tools that

12   one can use to scan the Internet for vulnerable computers,

13   so --

14   THE COURT: If you scan the Internet, how many

15   millions of computers are there?

16   THE WITNESS: There are a large number of computers

17   in the world, but there are tools that can scan the entire

18   Internet in less than an hour.

19   THE COURT: In less than an hour?

20   THE WITNESS: Yes, sir.

21   THE COURT: So what do you scan the Internet, and

22   what does it give you?

23   THE WITNESS: So there's a tool that was made by the

24   University of Michigan called ZMAP, Z-M-A-P, that can visit

25   and interact with every single computer on the Internet in

1   less than an hour. And think of it as knocking on the front

2   door of every house on the street.

3   THE COURT: What does it do?

4   THE WITNESS: It makes a connection to a computer,

5   and a follow-up activity would be looking for known flaws,

6   looking for likely methods of entry. So, you know, a

7   criminal might try and open the window on every front door --

8   or the front window of every house on the street.

9   THE COURT: So what you're saying is if they had

10 unlocked the computer, if they unlocked the door to this

11 house, a person could scan it, every computer in the world,

12 in one hour. And then what would that do?

13   THE WITNESS: They could gain access and do --

14   THE COURT: And do what?

15   THE WITNESS: Sorry?

16   THE COURT: How does it change what already has

17 occurred?

18   THE WITNESS: It's not that it changed what has

19 already occurred, it's that they could -- the information

20 that is on the computer could then be changed by subsequent

21 people entering the house.

22   THE COURT: The information on the computer. So the

23 information concerning the address would be changed?

24   THE WITNESS: Not the --

25   THE COURT: Right now we're talking about getting

1   the address or the computer of the individual concerned.

2   THE WITNESS: It's not --

3   THE COURT: It wouldn't change that, because the FBI

4   already has it, don't they?

5   THE WITNESS: The user name on the computer, the

6   identifiers, those wouldn't change, but any contraband the

7   government later discovered in an in-person search --

8   THE COURT: Well, first we're dealing with the

9   question of finding out whose computer it is that's

10   communicating with Playpen. They find that. Then you're

11   saying, well, they need to know the exploit, because it could

12   tell us what happened subsequent to that, correct?

13   THE WITNESS: Yes, Your Honor.

14   THE COURT: Couldn't tell us what happened before

15   that.

16   THE WITNESS: The -- so, as I said, there were two

17   main reasons for the defense to look at the exploit --

18   THE COURT: I understand that. They could put

19   something in there and put it into Tor -- into Playpen.

20   THE WITNESS: No. So the latter reason is the

21   reason -- as I just discussed, would go to what may have been

22   found on the computer weeks or months later.

23   The former reason, you know, knowing the state that

24   the computer is in, that goes to the validity of the

25   information that the NIT collects.

1   THE COURT: So what you're saying is that they

2   couldn't -- there's no way to rely on a name that they

3   obtain, and that would be wrong. Is that correct?

4   THE WITNESS: So there is a unique identifier on the

5   computer called a MAC address, and that was one of the things

6   collected by the NIT. It's a serial number for your Wi-Fi

7   card burned in at the factory. That can be changed by

8   software running on your computer, and so --

9   THE COURT: It can't be changed until you get to the

10   computer.

11   THE WITNESS: That is correct.

12   What I'm saying is if the exploit somehow

13   malfunctioned it's possible that that serial number might

14   have changed in such a way that it would be, you know,

15   forensically unreliable.

16   THE COURT: All right. Go ahead.

17   BY MR. GRINDROD:

18   Q. Let me ask you about the second reason you stated, which

19   was the one that had to do with changes to the computer

20   potentially after the NIT was deployed.

21   Does the time gap between when the NIT was deployed

22   and when the computer was physically seized in a traditional

23   search, does that affect anything as far as, you know, the

24   mistakes of that second reason?

25   A. There are a lot of criminals out there on the Internet

1   who try and break into computers, and the longer that a

2   computer is left vulnerable to cyber attackers the greater

3   opportunity those cyber attackers will have to compromise the

4   computer and use it for whatever purpose they have.

5   If someone -- you know, if the FBI were to show up

6   the day after the NIT operation, that would be a relatively

7   short window. If they waited a year or 11 months to conduct

8   the search, that would be a lot of time for a vulnerable

9   computer to be compromised by other third parties.

10 Q. Have you reviewed Agent Alfin's declaration in this case

11 that was also filed in the Matish case?

12 A. I have.

13 Q. So in paragraph 9 of that declaration Agent Alfin

14 essentially states that he executed the exploit and observed

15 that it didn't make any changes to the computer.

16   Do you have any views on that statement?

17 A. I do. I --

18   THE COURT: I -- well, go ahead. No objection?

19   MS. YUSI: (Shakes head.)

20   THE WITNESS: So Special Agent Alfin testified

21 saying, essentially, that the exploit worked just fine; that

22 he ran it on his computer a few times, it worked okay in the

23 lab, and there's no reason to believe that the exploit

24 malfunctioned and, as a result, there's no need for the

25 defense to be able to look at the exploit.

1   It's really hard to write reliable, secure software.

2   Large companies like Microsoft and Apple and Boeing, spend a

3   huge amount of money on software quality assurance, trying to

4   write code that does what they think it's supposed to do.

5   They also employ teams of people who do nothing but test the

6   software to look for flaws. And they don't just run it once

7   or twice, they run it thousands or millions of times, looking

8   for that one-in-a-million case where it misfires or does

9   something unpredictable.

10   It is frequently the case that software can have

11 subtle flaws that don't show up under a modest amount of

12 testing, and, you know, with respect to Special Agent Alfin's

13 declaration or testimony, running an exploit a couple times

14 is not enough to say conclusively that it works and that it

15 didn't have any bugs, particularly if he hasn't even looked

16 at the exploit, which is my understanding from that

17 testimony. You know, even when experts can look at codes,

18 sometimes they don't notice flaws. This is why we have, you

19 know --

20   THE COURT: So experts can differ.

21   THE WITNESS: Experts who have access to the same

22 information can differ, but in this case only one side has

23 access to the information, and we have to take their word for

24 what the code does.

25 BY MR. GRINDROD:

1 Q. So, Dr. Soghoian, let me direct your attention to another

2 component, which we talked about earlier, called the PCAP

3 data.

4   Now, in this same declaration that we were just

5 talking about, Agent Alfin's declaration, he, in paragraph

6 16, said that the data stream reflecting the information

7 transmitted to the FBI from the defendant's computer --

8   MS. YUSI: We object, Your Honor; leading.

9   THE COURT: Objection sustained. You may recite

10 exactly what he said.

11   MR. GRINDROD: Okay. Thank you, Your Honor.

12   THE COURT: Don't start summarizing --

13   MR. GRINDROD: I'm sorry. I was trying to --

14   THE COURT: -- because then you are changing, in

15 some ways, it. Let him understand what it is. You can say,

16 "He says as follows," and I'll allow you to do that, but

17 don't --

18   MR. GRINDROD: Thank you, Your Honor.

19   THE COURT: "In essence, he says this."

20   MR. GRINDROD: Thank you, Your Honor.

21   THE COURT: In essence, I might say one thing, but

22 the question is what it is that's exactly said.

23 BY MR. GRINDROD:

24 Q. So paragraph 16 of Special Agent Alfin's declaration

25 reads as follows:

1   "Review of this data stream reflecting the

2 information transmitted to the FBI from Matish's computer as

3 a result of the deployment of the NIT confirms that the data

4 sent from Matish's computer is identical to the data the

5 government provided as part of discovery."

6   Have you reviewed the PCAP data in Mr. Eure's case

7 and other Playpen cases?

8 A.   I have. I've reviewed the PCAP in this case and one

9 previous case.

10 Q.   In your view, is Special Agent Alfin's statement in

11 paragraph 16 that I just read to you -- is that statement

12 correct?

13 A.   No, in my view it is not. The PCAP -- the recording of

14 the data that the government received only shows what the

15 government received, it does not show what the NIT sent.

16   So think of it this way: You have someone putting a

17 letter in the mail, it goes through the U.S. Mail system, and

18 the government has a video camera pointing at the FBI's

19 office showing the letter being delivered. Their recording

20 doesn't show what happened along the way as the letter was

21 making its way from point A to point B, it doesn't show who

22 may have opened the letter, it just shows what happens once

23 the government has received --

24   THE COURT: So if you received any e-mails from

25 anyone it would have the same problem. It could be

1 different -- if you received it, it could be different from

2 what was sent, correct?

3   THE WITNESS: And, for that reason, there is

4 technology that you can use to protect against that.

5   THE COURT: I understand that, but I look at e-mails

6 all the time; I assume that they're what somebody sent. And

7 you're saying you shouldn't assume what somebody sent because

8 it could be changed along the way.

9   MR. GRINDROD: Can I follow up on that, Your Honor?

10   THE COURT: Certainly.

11 BY MR. GRINDROD:

12 Q. So clarify for me. Is this a theoretical possibility

13 that this information was changed, or can you testify that,

14 in fact, information in the PCAP data stream was changed?

15 A. Looking at the PCAP data stream, there are indicators in

16 there showing that at least some of the information was

17 changed as it was transmitted from A to B.

18   THE COURT: What was changed?

19   THE WITNESS: The IP address of the government

20 server that is in the PCAP recording is definitely not the IP

21 address that was -- that the NIT addressed the information to

22 when it left the defendants' computer.

23   THE COURT: Excuse me. The NIT addressed the

24 information to a different computer than that which was sent

25 back to them?

1   THE WITNESS: Your Honor, I'll try and explain it in

2   English to you, in plain English.

3   If I call your chambers --

4   THE COURT: Yes.

5   THE WITNESS: Let's say I have a telephone number.

6   I call your chambers, and I ask to speak to you.

7   THE COURT: Yes.

8   THE WITNESS: I'll speak to one of your colleagues,

9   and then they will transfer me on an extension to your

10 chambers.

11   THE COURT: Correct.

12   THE WITNESS: I may not know your direct line. In

13 the same way, the PCAP file does not have the extension of

14 the server that actually received the data -- sorry.

15   The PCAP file contains the extension number, it

16 doesn't contain the number of the main switchboard, and only

17 the main switchboard number was reachable from the outside

18 world.

19   THE COURT: So the government server that got the IP

20 or the exploit was not the government server that sent back

21 the information.

22   THE WITNESS: That's also true. There was a server

23 that the government maintained that delivered the exploit,

24 and then there was a different server that received the

25 information back from the NIT, but then there's also a third

1 government server --

2   THE COURT: Stop a minute.

3   First we have Playpen, okay?

4   THE WITNESS: That's a government server, yes, sir.

5   THE COURT: That's a government server. I thought

6 the exploit got you into the Playpen.

7   THE WITNESS: The exploit was delivered when someone

8 visited Playpen and caused the NIT to operate, which calls

9 home to a second government server.

10   THE COURT: Okay.

11   THE WITNESS: Then that second government server

12 passes the information to a third government server, and that

13 third government server's address is in the PCAP recording.

14   THE COURT: So, similarly, there are several

15 computers involved, is what you're saying.

16   THE WITNESS: The second IP -- the second server's

17 address, which is the one that the NIT would have called home

18 to, that never appears in the recording. So that IP address

19 was changed. As the information was being passed from server

20 number two to server number three the IP address was changed,

21 and the recording that we've been given only lists server

22 number three.

23   THE COURT: Okay. So the information being

24 transmitted back from the Playpen to the ultimate user of the

25 information -- that is, the person desiring the particular

1 documents or pictures that Playpen has -- it goes through

2 several different computers constantly in order to hide where

3 it came from or where it was going.

4 THE WITNESS: That is correct, Your Honor.

5 THE COURT: So this is not unusual, then, for

6 information to go from one computer to another.

7 THE WITNESS: If I might expand on what you're

8 asking, the ---

9 THE COURT: I'm merely asking how does the person

10 know that what they got is what was sent?

11 THE WITNESS: I have a good answer for that.

12 THE COURT: Oh.

13 THE WITNESS: So there's a technology called

14 "encryption." If you've ever visited your bank's Web site,

15 you'll see a lock icon, and that's designed to do two things.

16 It protects the confidentiality of information so that no one

17 can see your account number, but it also stops anyone from

18 tinkering with the information as it's sent from A to B. The

19 connection from Playpen to the visitors to the site was

20 encrypted, and so nothing could be tinkered with as it was

21 going from A to B.

22 The connection from the NIT users back to the FBI

23 was not encrypted, and so when the NIT called home the

24 government did not have a chain of custody of the data that

25 the NIT sent, and it could have been tampered with along the

1 way. Now, they knew how to maintain the chain of custody

2 because they used it for the outgoing data from the Playpen

3 site to the user, but they didn't use it on the way back.

4   And in your question about e-mails, it used to be a

5 big problem on the Internet that people would receive e-mails

6 that purported to be from other organizations. You could get

7 someone trying to steal your banking credentials by

8 pretending to be Bank of America or Chase. And now all of

9 the big Internet companies actually employ some encryption

10 technology that signs e-mails so that only Bank of America

11 can send e-mails that look like they come from Bank of

12 America, and if someone tries to fake it they go straight in

13 the trash can.

14 BY MR. GRINDROD:

15 Q. So I want you to imagine for me now that you were at

16 trial in this case and either Special Agent Alfin or some

17 other government expert testified, in sum and substance, to

18 what is in paragraph 16.

19   Would you testify to something inconsistent with

20 that?

21   MS. YUSI: Objection, Your Honor. This calls for

22 speculation as to --

23   THE COURT: I'm going to allow him to testify what's

24 wrong with it.

25   THE WITNESS: I disagree with Special Agent Alfin's

1   assessment of what the PCAP file -- what the recording shows.

2   I believe it does not show what the NIT sent, I believe it

3   only shows what the government received.

4   And, moreover, Special Agent Alfin --

5   THE COURT: So you can't tell what was sent

6   because -- you're saying the possibility that there was some

7   invasion or hacker that came in -- they could change whatever

8   was sent so that the identification of the computer of the

9   defendant was not the defendant's computer.

10   THE WITNESS: That possibility is there, and --

11   THE COURT: Except if they went to the defendant's

12   computer and saw it then it wouldn't make any difference to

13   you at all?

14   THE WITNESS: That's a legal question, Your Honor.

15   THE COURT: Oh, it's a legal -- what's legal about

16   it?

17   THE WITNESS: You're not asking me --

18   THE COURT: I'm asking you. You're the expert

19   testifying here, and I'm saying, as an expert, if the

20   information you received is what you saw, then you still feel

21   that a hacker changed it?

22   THE WITNESS: I'm not saying that a hacker has

23   changed this stuff, Your Honor, I'm saying that the

24   government had the means to maintain a chain of custody, and

25   they didn't use it.

1   THE COURT: Oh, unquestionably. I have the means to

2 maintain a lot of things that I don't maintain, and what

3 you're saying is in this case they didn't utilize encryption

4 in transmitting information. Is that correct?

5   THE WITNESS: That is true.

6   THE COURT: Okay. But that's not to say that the

7 information transmitted was incorrect, that's to say there's

8 a possibility that it could be incorrect if a hacker invaded

9 it and what they saw when they got there was different from

10 that which was transmitted.

11   But if it wasn't different...

12   THE WITNESS: So, separately, Special Agent Alfin

13 testified that the data that left the client is exactly the

14 data that was received by the government, and, as I just

15 testified before, the IP address information did change along

16 the way.

17   THE COURT: Okay. Go ahead.

18 BY MR. GRINDROD:

19 Q. So would you be able to have reached that conclusion had

20 you not analyzed the PCAP data?

21 A. No. Within five minutes of looking at the PCAP data it

22 was clear that there was something wrong, but without the

23 PCAP data the only thing I would have had to go on was

24 Special Agent Alfin's testimony saying that nothing changed.

25 Q. The question may come to someone's mind, why not conduct

1 a forensic analysis of the defendant's computer. So does

2 that move the ball forward one way or the other in answering

3 these questions that you've raised about the exploit?

4   MS. YUSI: Your Honor, I'm going to object. He's

5 not a forensic expert. He's talking about a NIT, and that's

6 his specialty.

7   THE COURT: He's a computer expert. I understand

8 that.

9   MS. YUSI: I'm not sure --

10   THE COURT: I'll allow him to testify as a computer

11 expert, not as a forensic expert.

12 BY MR. GRINDROD:

13 Q. Do you remember the question?

14 A. No. Can you say it again?

15 Q. Sure. So the question may come to mind, why not look at

16 our clients' computers.

17   THE COURT: Not "why not." Ask him a question.

18   MR. GRINDROD: Okay. So --

19   THE COURT: Don't ask him why not.

20   MR. GRINDROD: Okay.

21   THE COURT: Please, don't.

22 BY MR. GRINDROD:

23 Q. Would a forensic analysis of the hard drives of the

24 computers in this case --

25   THE COURT: Stop. He just said no forensic

1   testimony, and I agreed. He's not claiming to be a forensic

2   expert, he's claiming to be a computer expert, and you

3   just -- what a forensic -- do you see what I'm trying to tell

4   you? Let's don't get into that.

5   BY MR. GRINDROD:

6   Q. So you've addressed certain questions that -- and talked

7   about how the exploit may shed light on certain answers. Is

8   there anything about looking at the computers themselves in

9   this case that would answer those same questions?

10   A. It would be very difficult. The longer the time period

11   between when the NIT and the exploit executed and when the

12   computer was searched and ultimately a forensically sound

13   copy of the computer was made -- the longer that period is,

14   the more time there is for information on that computer to

15   deteriorate.

16   If the government had conducted the search of the

17   defendant's house an hour after the NIT operated and the

18   computer hadn't been turned off, you know, you'd probably

19   have a pretty good idea of what happened. But if it's been

20   months and the computer has been turned off frequently, a lot

21   of information would have been lost, particularly if much of

22   what the NIT and the exploit did only tampered with the

23   software that was running on the computer and not the

24   software that was installed permanently on the computer.

25   And, so, it would be really hard to reconstruct what

1   happened a year before just by looking at the physical

2   computer, without being able to look at the individual

3   components of the government's software that ran on the

4   computer.

5   Q. Let's talk quickly about the last component that has not

6   been produced, the unique ID generator.

7   You told us what that is, but can you tell us why

8   that's important, from your technological perspective?

9   A. Sure. As I said before, the purpose of the ID generator

10 is to allow the government to associate a known user on the

11 Web site, someone with user name Jack, with a particular IP

12 address that is revealed through the NIT.

13   For that to be -- for the ID generator to be

14 helpful, it must generate a unique ID only once. If it

15 malfunctions for some reason and generates the same ID over

16 and over again, you could incorrectly associate one user's

17 activity on the site with a different person's IP address.

18 Q. Other than looking --

19   THE COURT: Well, was there any evidence that there

20 was multiple deliverance of the same site?

21   THE WITNESS: Well, there's certainly hundreds --

22   THE COURT: I didn't ask you that. Was there any

23 evidence in this case? I don't remember any declaration

24 saying that. Where do we get this? Is there any evidence of

25 this?

1   MR. GRINDROD: I'm sorry. Any evidence of what,

2   Your Honor?

3   THE COURT: Just what he testified to.

4   MR. GRINDROD: Well, Your Honor, we haven't been

5   provided with the evidence. We haven't been provided with a

6   unique identifier, so we don't --

7   THE COURT: Well, how is he testifying as an expert

8   on that which he doesn't know any evidence of?

9   MR. GRINDROD: He knows what --

10   THE COURT: It makes suppositions, but I don't want

11 to start talking about evidentiary matters. When we start

12 dealing in that we're dealing in a different scope. He's an

13 expert. Not a forensic expert, but a computer expert. And I

14 am assuming that he is a computer expert.

15   MR. GRINDROD: Well, this --

16   THE COURT: The question in my mind is -- the only

17 question I'm trying to find out is where we're going.

18   MR. GRINDROD: I --

19   THE COURT: The question really before us is did the

20 government violate Mr. Eure's constitutional rights.

21   MR. GRINDROD: Well, Your Honor, we're --

22   THE COURT: That's one question we're dealing with,

23 and so far I've heard very little about that. I've heard a

24 lot about the computer. So eventually we're going to start

25 talking about something that's evidentiary in this case.

1   We allowed an expert to testify, and I did it out of

2 order, without any evidence at all other than the evidence in

3 the declarations. And we can do that because this is not a

4 trial of any sense but a question of the appropriateness of

5 various search warrants.

6   MR. GRINDROD: Well, Your Honor, we're also --

7   THE COURT: And I assume we are dealing first with

8 Mr. Eure's warrant that you're trying to suppress the

9 evidence. Now, what evidence are you trying to suppress?

10   MR. GRINDROD: None with this, Your Honor. I'm

11 sorry. As I tried to flag for the Court, I had moved on to

12 the motion to compel. These are trial --

13   THE COURT: Oh, you're not -- the only thing in the

14 motion to suppress, then, was what was on his computer?

15   MR. GRINDROD: Was the -- well, Your Honor, to the

16 extent -- Your Honor, basically, the testimony that I offered

17 with respect to where the NIT was installed, the geographic

18 location, and also as to how the NIT would have worked had

19 the warrant only authorized it being deployed on computers

20 that were located in the Eastern District of Virginia. Those

21 were the topics that were specifically directed to the

22 suppression.

23   THE COURT: So all of this testimony that he has,

24 other than that very short testimony, deals with the motion

25 to compel.

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

2   THE COURT: I got lost on the motion to suppress.

3   And so all of this deals with the motion to compel them to

4   produce what?

5   MR. GRINDROD: To produce the exploit and the unique

6   ID generator.

7   THE COURT: The code is what you want, correct, the

8   code that allows them to get into Tor?

9   MR. GRINDROD: The code that allowed them to get

10   into our client's computer. They were operating the Playpen

11   server on Tor, but --

12   THE COURT: So what you're seeking to suppress is

13   exactly what? So tell me.

14   MR. GRINDROD: Well, with respect to suppression,

15   it's everything that was a fruit of the NIT.

16   THE COURT: Everything is nothing, so tell me what

17   it is you're seeking to suppress.

18   MR. GRINDROD: Your Honor, we're seeking to suppress

19   all fruits of the NIT search. And that's how they identified

20   our clients in these cases, so it's everything. I mean, I

21   don't mean to be cavalier --

22   THE COURT: Well, normally if we have a weapon we

23   want to suppress the utilization of the evidence.

24   MR. GRINDROD: Correct.

25   THE COURT: If it's the subject of a seizure, that

1 was the subject of an illegal search and seizure. Evidently,

2 they seized or obtained evidence by a search.

3   MR. GRINDROD: That's correct.

4   THE COURT: And you're seeking to suppress what?

5 That's all I'm asking.

6   MR. GRINDROD: To suppress the evidence of the --

7 obtained by -- I'm sorry, Your Honor.

8   THE COURT: What evidence? What gun, weapon,

9 anything else? Tell me what it is you're seeking to

10 suppress.

11   MR. GRINDROD: We're seeking to suppress the hard

12 drives, the -- we're seeking to suppress the information --

13   THE COURT: The hard drive is not in evidence. It's

14 not -- what difference does that make? It's what information

15 was taken from the hard drive.

16   MR. GRINDROD: Any and all evidence from it, Your

17 Honor.

18   THE COURT: What information are you seeking to

19 suppress, is what I'm trying to get at.

20   MR. GRINDROD: If I could --

21   THE COURT: When we suppress something we have an

22 object to suppress; a PIN, the wording of such-and-such and

23 so-and-so, this particular evidence.

24   All I'm asking is what evidence are you seeking to

25 suppress?

1   MR. GRINDROD: We're seeking to --

2   THE COURT: When you say, we're seeking to suppress

3 all evidence of his guilt, that's wonderful, but it doesn't

4 help me a bit. It doesn't help anyone.

5   So what are we seeking to suppress?

6   MR. GRINDROD: Testimony about our client's alleged

7 activity on the Playpen Web site, testimony regarding -- Your

8 Honor --

9   THE COURT: That's not a motion to suppress. You've

10 got to suppress some evidence. What evidence are you seeking

11 to suppress?

12   MR. GRINDROD: The IP address mainly, Your Honor.

13   THE COURT: I understand you're seeking to suppress

14 anything that might lead to your client being guilty, and I

15 understand that, but that is not a motion to suppress.

16 You've got to suppress something.

17   MR. GRINDROD: We're seeking to suppress the IP

18 address, the MAC address --

19   THE COURT: Wait a minute. You're seeking to

20 suppress the IP address of the defendant, correct?

21   MR. GRINDROD: Correct.

22   THE COURT: What else?

23   MR. GRINDROD: The MAC address.

24   THE COURT: The MAC -- what's the MAC address?

25   MR. GRINDROD: It's the unique code that appears on

1   any wireless card, so it would have been the code associate

2   with the device our client used to access the Internet. It

3   was obtained through the use of the NIT.

4   THE COURT: You're trying to suppress what your

5   client's code was?

6   MR. GRINDROD: Yes, Your Honor.

7   THE COURT: Client's code.

8   MR. GRINDROD: The host name, Your Honor, the

9   operating system.

10   THE COURT: You can't suppress a system. You can

11   suppress something.

12   MR. GRINDROD: Suppress any testimony regarding what

13   operating system was running on any computer associated

14   with --

15   THE COURT: You want to suppress any evidence of any

16   operating systems on any computer or a particular computer?

17   MR. GRINDROD: On the computers mentioned in the

18   forfeiture allegations in this case.

19   If I may, Your Honor, I don't mean to make an end

20   run at all around the Court's desire to get specific about

21   this, but if I could just very briefly explain why I think it

22   is -- why the --

23   THE COURT: No, don't explain anything. The witness

24   is on the stand. Let's keep going.

25   MR. GRINDROD: Understood, Your Honor.

1   THE COURT: You've got five minutes, and that's it.

2   MR. GRINDROD: Understood, Your Honor.

3   THE COURT: The ball game's over.

4 BY MR. GRINDROD:

5 Q. We were talking about the unique ID generator. Is there

6 any other means of determining whether multiple IDs were

7 created that matched, other than having the generator itself?

8 A. The government's server would know which IDs were sent

9 back, so the government has in their possession a list of NIT

10 clients that called home and what their unique IDs were. But

11 some of the NIT clients would never execute properly, so

12 there would be failures. And so there's no way of knowing,

13 without looking at the generator, if the generator would have

14 executed successfully, if it did what it was supposed to do

15 and gave unique codes to everyone.

16   THE COURT: What is the ID generator?

17   THE WITNESS: So this is the code that creates

18 serial numbers for each operation of the NIT.

19   THE COURT: "This is the code." The ID generator is

20 the code?

21   THE WITNESS: Yes, Your Honor.

22   THE COURT: So without knowing the code you don't

23 know what the government's position was.

24   THE WITNESS: Without knowing the code you don't

25 know if the ID numbers were created properly. In a

1 successful, good operation you would want one new code for

2 each delivery of the NIT. If that code malfunctioned and

3 gave two people the same ID, that would be a bad thing.

4   THE COURT: Except we have no evidence of any

5 malfunction. That's a supposition you're making. If that

6 occurred something would be different, correct?

7   THE WITNESS: That's why it's useful to have the

8 code.

9   THE COURT: If it occurred, something would be

10 different, correct?

11   THE WITNESS: Yes, Your Honor.

12   THE COURT: All right.

13 BY MR. GRINDROD:

14 Q. Let me jump back and talk to you briefly about the

15 exploit one more time.

16   To your knowledge, has the FBI disclosed the exploit

17 in this case to anyone?

18 A. Sure. When the operation took place the government would

19 have provided the exploit to hundreds of thousands of people.

20 When the operation took place the exploit was delivered to

21 every person who the government delivered the NIT to.

22 Q. Was there any way for someone to capture the exploit or

23 record it?

24 A. Sure. Just as the government can make a recording, a

25 PCAP file, on their end and record the data that they

1   receive, so, too, can individuals record a copy of all the

2   data that they receive from the Web sites that they visit.

3   And in a previous NIT operation that the government

4   did in 2013 a copy of the exploit that they used then was --

5   the exploit and the NIT were saved by experts who visited the

6   Web site that was being used for the NIT delivery, and the

7   government's exploit and NIT were analyzed by independent

8   experts.

9   So the government has in the past, through

10   unfortunate luck, had their NIT and their exploit analyzed by

11   the open research community.

12   THE COURT: This particular NIT was -- this exploit

13   was analyzed?

14   THE WITNESS: No, Your Honor, a different one that

15   they used in --

16   THE COURT: A different exploit.

17   THE WITNESS: -- in 2013.

18   THE COURT: In 2013.

19   THE WITNESS: This operation took place in 2015, but

20   two years before that the FBI seems to have made a mistake,

21   and their NIT was delivered to people who were not themselves

22   viewing contraband, and some of those individuals saved

23   copies of the NIT and published it online.

24   MS. YUSI: Your Honor, I'm going to object to his

25   speculation as to any mistake that was made.

1   THE COURT: I'm going to allow him to testify for

2   what it's worth, ma'am, okay? Let's go.

3   MR. GRINDROD: I have no further questions at this

4   time, Your Honor.

5   THE COURT: All right. You have 50 minutes for

6   cross-examination. We're going to have to come back tomorrow

7   morning, it looks like.

8   MS. YUSI: I'm sorry, Your Honor. You said we only

9   have 15 more minutes?

10   THE COURT: 50 minutes.

11   MS. YUSI: Okay, Your Honor.

12   THE COURT: Wait a minute.

13   Mr. Cejas, in relation to your portion of this

14 testimony, do you want to ask any more questions of this --

15   MR. CEJAS: No, sir.

16   THE COURT: All right. Anything that hasn't been

17 asked. All right. Let's go.

18   MS. YUSI: Your Honor, I have an agent here. I have

19 Special Agent Alfin here from D.C., so I'm hoping we can get

20 him on briefly today.

21   THE COURT: Okay.

22   CROSS-EXAMINATION

23 BY MS. YUSI:

24 Q. Dr. Soghoian, you said you're pro bono here, but you're

25 not here on behalf of the ACLU, correct?

1 A.   That's correct.

2 Q.   Do they support you being here?

3 A.   What does that mean?

4 Q.   I mean, did they approve? Did you ask to be here on

5 their behalf?

6 A.   Not on their behalf. I was told, in fact, that for the

7 NIT work that I've been doing, the unpaid NIT work, that I

8 should emphasize in each case that I'm doing this in my

9 personal capacity and not on behalf of the ACLU.

10 Q.   Okay. Your supervisors told you to not associate the

11 ACLU with what you're here for today?

12 A.   And when I speak on panels at conferences I'm also told

13 to say that, just like government employees.

14 Q.   All right. Now, you agree that the TOR project doesn't

15 promise perfect security to its users, correct?

16 A.   I believe there's a statement on the Tor Web site that

17 acknowledges risks associated with the Tor software, yes,

18 ma'am.

19 Q.   And Tor is used by a lot of people, but it includes

20 criminals who commit crimes, correct?

21 A.   I believe that's true.

22 Q.   Do you believe that, or do you know that to be true?

23 A.   I don't know any criminals that have used Tor, but --

24 Q.   But you've testified in a lot of criminal -- well, this

25 particular --

1 A.   This is my third case.

2 Q.   Okay. But you're aware that Tor has been used by

3 criminals, based on news reports and things like that.

4 A.   Yes, ma'am.

5 Q.   Okay.

6   THE COURT: You didn't know that child pornography

7 was criminal?

8   THE WITNESS: I'm aware that child pornography is a

9 crime, but I don't have firsthand knowledge -- I only have --

10 I've read the newspapers --

11   THE COURT: You don't have firsthand knowledge of

12 any of this, sir, you only have knowledge that was based on

13 what your investigation was. And your investigation did not

14 reveal any criminal activity?

15   THE WITNESS: The --

16   THE COURT: You mean you didn't see anything about

17 child pornography in this case?

18   THE WITNESS: Your Honor, I haven't looked at any

19 child pornography in this case.

20   THE COURT: Nobody told you what this case was

21 about?

22   THE WITNESS: I've certainly read the affidavits in

23 this case, but I haven't looked at any of the child

24 pornography, if that's what you're asking.

25   THE COURT: The affidavits mean nothing. That's the

1   evidence in this case, correct?

2   THE WITNESS: The --

3   THE COURT: You didn't analyze anything from the

4   affidavits. Even as a human being you didn't realize that

5   this was all dealing with child pornography?

6   THE WITNESS: So my understanding -- so the three

7   cases --

8   THE COURT: Your understanding is child pornography

9   is not a crime?

10   THE WITNESS: Your Honor, the three --

11   THE COURT: You testified that this wasn't criminal

12   activity.

13   THE WITNESS: The three cases in which I've

14   testified, none of them have led to convictions yet, so I

15   don't personally know --

16   THE COURT: So it's not a crime unless someone is

17   convicted of it, correct?

18   THE WITNESS: I'm not a lawyer, Your Honor, but

19   that's --

20   THE COURT: Just so I understand what you're

21   saying -- you know, the problem is -- the only thing that's

22   criminal is if there's a conviction? If somebody shoots

23   another person and they don't convict them, it's not

24   criminal, correct?

25   THE WITNESS: I don't know, Your Honor. I'm not an

Heidi L. Jeffreys, Official Court Reporter

1 expert on that.

2   THE COURT: You don't have to be an expert to

3 understand what murder is, do you?

4   THE WITNESS: (No answer.)

5   THE COURT: You know, I'm not trying to do anything

6 except find out...

7   Go ahead. I'm sorry, Ms. Yusi.

8 BY MS. YUSI:

9 Q. You agree that law enforcement -- their job is to stop

10 crime, correct?

11 A. That is one of their jobs, yes, ma'am.

12 Q. All right. And they have an obligation to stop crimes,

13 including sexual exploitation of children on the Internet.

14 A. Yes, ma'am.

15 Q. And they need to stop and identify these criminals

16 through legally available means, correct?

17 A. I'm sorry. Can you ask that question again?

18 Q. Do you agree that law enforcement should stop the

19 exploitation of children on the Internet through legally

20 available means? Do you agree with that?

21 A. Yes, if those means are lawful.

22 Q. Okay. But you also agree that your purpose is to also

23 fight government surveillance, right?

24 A. Yes, ma'am -- well, I believe that my role is to help our

25 democratic system keep surveillance under control.

1   Q.   Okay. And to fight surveillance?

2   A.   That is what I do through my actions as someone who helps

3   the courts and legislative bodies adequately oversee

4   surveillance tools that are frequently used in the shadows.

5   Q.   And you consider yourself an activist, correct?

6   A.   I'm an activist and a scholar and a researcher.

7   Q.   Okay. I'm going to show you what I've marked as

8   Government's Exhibit 1.

9   THE COURT: Ms. Yusi, I'm going to keep going until

10   the government testifies, so everybody just be prepared to

11   stay late.

12   MS. YUSI: Thank you, Your Honor.

13   BY MS. YUSI:

14   Q.   Do you recognize this?

15   A.   Yes, ma'am.

16   Q.   What is it?

17   A.   These appear to be printouts of tweets of mine from

18   Twitter.

19   Q.   And what is Twitter?

20   A.   Twitter is a social network.

21   Q.   Okay. And you have an account there?

22   A.   Yes, ma'am.

23   Q.   And you frequently tweet about personal and professional

24   observations?

25   A.   It's mainly professional.

1 Q. Mainly professional.

2 A. Uh-huh.

3 Q. This is the front page of your Twitter account, correct?

4 A. That is my Twitter home page, yes, ma'am.

5 Q. And how do you describe yourself?

6 A. In my bio it says I fight surveillance, and then it says,

7 "Views expressed here are my own," which, as I described

8 before, my employer asked me to put.

9   And then -- do you want me to continue?

10 Q. No, that's okay.

11   And I'm going to show you page 2 --

12   MS. YUSI: I'm sorry, Your Honor. The government

13 moves to admit Exhibit 1.

14   THE COURT: You're going to have to speak into the

15 microphone.

16   MS. YUSI: I'm sorry, Your Honor.

17   The government moves to admit Exhibit 1.

18   THE COURT: This is merely for what purpose, ma'am?

19   MS. YUSI: Your Honor, bias, to show the expert's --

20   THE COURT: Has he admitted to this?

21   MS. YUSI: He admitted that these are tweets that he

22 wrote on his Twitter account.

23   THE COURT: All right. It's admitted, but I haven't

24 looked at it yet, other than the front page of this thing.

25   MS. YUSI: I'll go through it, Your Honor.

1   THE COURT: Okay.

2   (The exhibit was admitted into evidence.)

3   BY MS. YUSI:

4   Q. Page 2. Is this one of your tweets?

5   A. Yes, ma'am.

6   Q. And what did you say?

7   A. Are you asking me to read it, or --

8   Q. I am asking you to read it.

9   A. So this is a tweet @daveaitele, who is an ex-NSA analyst.

10   "The FBI shat the bed with their Playpen op. An

11 overbroad, illegal warrant, and no chain of custody for the

12 data they collected."

13 Q. At this point had you looked at things on some of these

14 defendants' computers?

15 A. I've never looked at any defendant's computer, ma'am.

16 Q. I'm talking about the information that was sent. Had you

17 looked at the NIT and the source code and the affidavit or

18 the search warrant? At this point had you looked at those?

19 A. What is the date of this tweet?

20 Q. I'm not sure. You remember writing it, though, so --

21 A. That's because I was shown it in court last week.

22 Q. Okay. And at that point you said you didn't remember,

23 right?

24 A. I didn't remember if I had tweeted it, but then one of

25 your colleagues from the U.S. Attorney's Office in Arkansas

1 | showed me a printout, and I believe I said, "That looks about

2 | right."

3 | Q. Okay. And do you remember the date?

4 | A. No.

5 | Q. So you're not sure if you had this opinion before or

6 | after you started testifying?

7 | A. Testifying or looking at stuff?

8 | Q. Either.

9 | A. Well, I testified in the *Michaud* case, which was the

10 | first one, but never looked at the NIT or the PCAP file. I

11 | never looked at any of the evidence that was under protective

12 | order in that case. I only looked at that in the Arkansas

13 | case, in which I testified two weeks ago.

14 | Q. But you have an opinion that everything that the FBI did

15 | in this case, or the NIT, was illegal, correct?

16 | A. I have a personal opinion that the method that the

17 | government employed exceeded Rule 41 of the Rules of Criminal

18 | Procedure and that it has some serious Fourth Amendment

19 | issues to it, yes, ma'am.

20 | Q. Okay. And you want to see the source of all this in

21 | order to further show that you believe it's illegal, correct?

22 | A. No. I believe that the legal issues can -- the Rule 41

23 | issue I believe doesn't involve the source code. I believe

24 | that the Fourth Amendment issue as to whether searching

25 | 10,000 or 50,000 computers with a single warrant -- whether

1   that -- I don't think the code is important there.

2   I think in this case, you know, if you -- there are

3   things that the defense counsel, I think, wants to be able to

4   see, such as the chain of custody, such as the state that the

5   computer was in before it was hacked, the state the computer

6   was in after it was hacked, where the code would be useful.

7   I'm actually, as I -- I assume you've read the

8   Arkansas transcript. As I said there, I'm actually not the

9   right person to look at the exploit itself. I don't want to

10 look at the exploit. I don't have the skills for it. In the

11 same way you wouldn't hire a tax attorney to do a murder

12 defense, I don't have the specialized skills to look at the

13 exploit.

14 Q. So you want to be -- just to be clear about your position

15 just in general, you want to fight surveillance and limit the

16 government's ability to surveil on the Internet, including

17 Tor?

18 A. I believe in the Fourth Amendment, and the Fourth

19 Amendment limits the role of government, and the Fourth

20 Amendment creates a role that judges have to play of

21 supervising surveillance tools, and I think that it would be

22 a really awesome thing if the Fourth Amendment more robustly

23 were applied to the use of NITs.

24 Q. So the Fourth Amendment was violated in this case, and

25 you believe that without even having seen what you call the

1 whole NIT in this case.

2 A. So, as I said before, in my view there are real questions

3 about whether a single warrant can be used to authorize

4 50,000 or 100,000 searches.

5   THE COURT: Were there 50,000 users of this child

6 pornography site? Is that what you're saying?

7   THE WITNESS: The FBI has testified that there were

8 100,000 people who visited the site in the two weeks that it

9 was under the government's control, but they have not

10 revealed how many of those were --

11   THE COURT: 100,000?

12   THE WITNESS: Yes, Your Honor, but they have not

13 revealed how many of those the NIT successfully operated

14 against.

15   THE COURT: 100,000?

16 BY MS. YUSI:

17 Q. And if there were 100,000 people, you agree that law

18 enforcement still has an obligation to try to investigate who

19 is a part of this Web site, correct?

20 A. Sure.

21 Q. And regardless of how many there are, if it's a legal

22 warrant then it's a legal warrant, correct?

23 A. No. I think that -- I think that the Fourth Amendment --

24 the Fourth Amendment should not permit searches of such a

25 huge scope. I think that if -- with a single warrant the

C. Soghoian - Cross

1 government can search thousands of computers --

2 Q. But this personal opinion -- I mean, you have this

3 opinion, and you're applying it to see the -- you want the

4 NIT released, correct, in an effort to further your personal

5 opinion.

6 A. I don't know that anyone is asking for it to be released,

7 ma'am.

8 Q. You're asking for access to it, and that's to further

9 your personal opinion, correct?

10 A. I haven't asked for access to the NIT for my sake,

11 because I don't have the skills to look at the exploit. The

12 NIT has already been turned over to the defense.

13 Q. Okay.

14 A. The exploit is something that I don't have the skills to

15 analyze.

16 Q. But you're opining as to why it would be important.

17 A. Sure, but whoever will look at that will be under a

18 protective order, just like I'm under a protective order for

19 the NIT.

20 Q. And you also criticize the FBI publicly on a regular

21 basis. Is that right?

22 A. As I also criticize companies and other parts of the

23 government, yes, ma'am.

24 Q. Let me show you page 3 of Exhibit 1.

25   And you're criticizing the FBI for saying that they

1   can't be bothered to use security, a secure Web site,

2   correct?

3   A.   Yes, ma'am.   Would you like me to describe that?

4   Q.   No.

5   A.   Can I?

6   Q.   I haven't asked that question, but --

7   A.   Well, may I describe what I'm saying here?

8   Q.   Sure.

9   A.   Okay.   Last year the Office of Management and Budget

10 required every federal agency to encrypt their Web sites. By

11 default, the FBI home page is now encrypted, as are many U.S.

12 Government agencies.

13   Over the last few months and the last year, I have

14 pushed different parts of the government to follow that

15 order, and I have had personal conversations with the FBI's

16 general counsel about encrypting their e-mails, for example,

17 and they say that they're working on that.   They're making

18 slow progress, and I think that, just as the FBI has

19 encrypted its home page, they should be using encryption on

20 their NIT server.

21 Q.   Let me show you what's been marked as --

22 A.   Ma'am, there are no page numbers on this, so --

23 Q.   Right.   That's why I'm counting.   Page 6, where it starts

24 with, "The FBI's malware transmits data back to the FBI

25 server."   And it will be on your screen, too.

1   A.   Okay.

2   Q.   Do you see that?

3   A.   Yes, ma'am.

4   Q.   So, again, you're commenting on the FBI, and what does

5   "face palm" mean at the end?

6   A.   "Face palm" is a way of expressing shock at an action.

7   Q.   That means -- okay. So you're, once again, commenting

8   on --

9   A.   So this is -- embedded under that tweet is a screenshot

10 from -- wait a minute. I haven't seen this in a while.

11   (There was a pause in the proceedings.)

12 BY MS. YUSI:

13 Q.   You're commenting on the Matish case here, correct?

14 A.   That's correct.

15 Q.   And that's the other case in this court in front of Judge

16 Morgan. Is that correct?

17 A.   This would have been a public document, and I was

18 embedding a screenshot from a public document and summarizing

19 for a lay audience what that document said.

20 Q.   So you're advertising what you're doing on your behalf in

21 your pro bono as an expert, correct?

22 A.   No, I'm describing facts that have come to light in

23 public proceedings.

24 Q.   Okay. And you're also bragging about providing

25 declarations and things like that in these cases, correct?

1   A.   What do you mean by --

2   Q.   I'm going to show you -- you can look on the screen, too.

3   "I wrote an 8-page expert declaration in an FBI

4   hacking case." And you --

5   A.   I don't see anything there that's bragging.

6   Q.   If you can look on the screen --

7   A.   No, I see the tweet. I'm saying I don't see that as

8   bragging. I'm publishing a link to a copy of a declaration

9   that I downloaded from PACER, which is a publicly accessible

10 system. I paid for the declaration through PACER and

11 published it because there are a number of scholars, academic

12 scholars, and journalists who are really interested in

13 NIT-related issues.

14 Q.   Okay. And this is your livelihood, correct? I mean, you

15 want to continue this livelihood after this case is over,

16 correct?

17 A.   So the way it works at the ACLU is I'm actually not told

18 what to work on. So no one said, "Chris, please spend time

19 on NITs."

20   I think this is interesting, so I chose to work on

21 this. There are a million other issues I could work on.

22 There's no shortage of interesting Fourth Amendment issues,

23 and so if the entire NIT issue went away I would move on to

24 body cams or GPS darts or whatever new surveillance

25 technology the government uses. There are plenty of people

1 who want to learn how they work and have me explain it to

2 them.

3 Q. Okay. And, as you said, you fight surveillance, and

4 particularly government surveillance is what your main focus

5 is.

6 A. I mean, I worked in consumer privacy issues for a few

7 years, but I've shifted my work towards government issues,

8 yes, ma'am, the U.S. Government but also other governments.

9 Q. I want to talk to you about your declaration and some of

10 the things you were testifying about earlier.

11 A. Sure.

12 Q. Do you have a copy of your declaration?

13 A. I don't. Do you have a spare copy that you could give

14 me?

15 Q. Yes.

16   (There was a pause in the proceedings.)

17 BY MS. YUSI:

18 Q. I'm going to show you what we marked as Government

19 Exhibit 2.

20   MS. YUSI: Your Honor, this is just a copy of -- I

21 don't know if I need to admit it into evidence, but I will do

22 so now, the declaration of Dr. Soghoian, just for ease sake.

23   THE COURT: Was it attached to --

24   MS. YUSI: It was attached to the reply in support

25 of Defendant Eure's motion to compel.

1   THE COURT: Okay.

2   (The exhibit was admitted into evidence.)

3 BY MS. YUSI:

4 Q. If we could look at paragraph 19 on page 5.

5 A. Yes, ma'am.

6 Q. And that's where you're criticizing the FBI about not

7 using encryption for information that was transmitted by the

8 NIT to the FBI server, correct?

9 A. Yes, ma'am, that's true.

10 Q. Now, when you talk about how someone could possibly have

11 tampered with that information, that's speculation, correct?

12 A. Sure.

13 Q. Okay. There's no proof of any of that in this particular

14 case, correct?

15 A. It is very difficult to detect tampering with unencrypted

16 data as it goes over the Internet.

17 Q. So it's just speculation that you might be able to see

18 something when you looked at it, correct?

19 A. When you say "you" do you mean me, or do you mean someone

20 watching the data as it's going over the network?

21 Q. I'm talking about you looking at the exploit or the

22 unique identifier that you want to look at.

23 A. The unique identifier and the exploit have nothing to do

24 with encryption issues.

25 Q. Okay. All right. So --

1 A. The encryption issue is about chain of custody --

2 Q. Okay.

3 A. The exploit is about the state of the computer and

4 whether the information derived from it was forensically

5 sound.

6 Q. Okay. How would it work? Do you know how it would work

7 if someone had -- what would have to happen if someone was to

8 have changed the information that was sent from the user back

9 to the FBI?

10 A. Sure, I can explain that. So when data is sent over the

11 Internet it goes from your computer to a remote server, say

12 the FBI's Web site, and it has to -- we don't have direct

13 connections, direct lines, from, you know, our houses to

14 every Web site we visit. We have to go through a bunch of

15 points along the way, and those points are servers or devices

16 that are called routers that are run by companies like

17 Comcast, Verizon, and AT&T. And at every point along the

18 path anyone controlling that server, either the operator of

19 the network or a hacker or a foreign government that has

20 gained improper access to those devices --

21 Q. Are you saying that a foreign government is involved with

22 hacking this particular case?

23 A. I don't know, but I -- would you like me to finish what

24 I'm saying, or --

25 Q. No, I'm just -- you're saying a lot, so I'm trying to --

1   A.   Governments hack routers. This is a known thing. The

2   U.S. Government hacks foreign communications networks, and

3   I'm sure that China and Russia hack U.S. Government networks.

4   This is why there are a lot of people working in cyber

5   security these days.

6   Generally, servers that deliver our data are not

7   trusted anymore. This is why large responsible organizations

8   now use encryption to protect data. This is --

9   Q.   And I get that, but what I'm asking for is the NIT was

10   sent to a user's computer, correct? And then that NIT got

11   the information from that computer and sent it to the FBI

12   immediately, correct?

13   A.   I mean, there might have been a one-second delay, I don't

14   know, but quickly.

15   Q.   Someone, if it was unencrypted, would have to hack it or

16   be involved with it during that one second, correct?

17   A.   No.

18   Q.   No?

19   A.   No.

20   Q.   Okay. So --

21   A.   If they had already hacked the server and they had --

22   Q.   Hacked the FBI's server?

23   A.   No, ma'am, hacked one of the servers or routers sitting

24   between an individual NIT user and the government server.

25   Either someone who has hacked it, an employee or a piece of

1 malfunctioning software on one of those computers, could

2 change data that is going through it, just as the

3 government's own server changed the IP address in the PCAP

4 file that you gave to me.

5 Q. Okay. Well, the PCAP -- let's talk about that.

6   You're talking about something that was -- you're

7 talking about the review of the PCAP data indicated that

8 the -- seized from the defendant's computer changed in

9 transit, correct?

10 A. Uh-huh.

11 Q. When you're talking about that, are you talking about the

12 substantive data or the header that was sent back?

13 A. The IP address appears in the header, not the -- if you

14 have, like, the envelope and the data that's inside the

15 envelope, it would be the data on the outside of the envelope

16 that was changed.

17 Q. So it's like the header of an e-mail. Like when you

18 reply to something you don't change the subject, but it says

19 "Re," R-E. When you reply to most e-mails accounts it

20 automatically does that on the header, correct?

21 A. I don't think that's a great analogy. I think -- I mean,

22 there are other ones that I --

23 Q. I'm just saying it's the automatic change of a header as

24 it goes through.

25 A. Certainly, the two changes that definitely occurred here

1 were automatic. We have no way of knowing if there were any

2 other changes, because you didn't use encryption.

3 Q. So when you're telling the Court that you found

4 indications that something was tampered with, you were

5 talking about automatic changes.

6 A. I'm saying that the data in the PCAP file is not the same

7 information that left the defendant's computer.

8 Q. Because of automatic changes in the header.

9 A. So it was changed probably by the Wi-Fi router in the

10 defendant's home, and that would have been a change of the

11 source address. And then whatever government server was --

12 Q. I'm asking -- it was automatic, correct?

13 A. Yes.

14 Q. And you want the Court -- you were trying to have the --

15 your information to the Court was automatic changes mean that

16 that's evidence that there could be other changes in the

17 substantive. Did you find any changes in the substantive?

18 A. No. This is the -- the IP address isn't in the

19 substantive part, the IP address appears in the header.

20 Q. I'm talking about the substantive portion. You found

21 nothing different in that from what was sent to the user to

22 what was sent back to the FBI.

23 A. We don't know what --

24 Q. You looked at the PCAP.

25 A. Right. That only shows what was received by the FBI.

1   Q.   Okay.

2   A.   It doesn't show what left the user's computer.

3   Q.   You saw the unique identifier in both what was sent to

4   the computer and what was received by the FBI. Is that

5   right?

6   A.   I saw the unique identifier that was received by the

7   PCAP -- that is contained in the PCAP file.

8   Q.   So just to be clear, there are no substantive changes.

9   You saw automatic changes, and that is what you're relying on

10 to say that there's a possibility that there were other

11 changes.

12 A.   I think that's not a great way of saying it. You didn't

13 give me --

14 Q.   Is that a simple way to say it?

15 A.   No. You didn't give me two PCAP files. It's not like I

16 looked at one file and looked at another and saw something

17 change from A to know B. All you gave me was one file, but I

18 can tell from the IP addresses that are in it that it was

19 changed twice.

20 Q.   And wasn't it a two-way communication file?

21 A.   That's what the government called it, yes, ma'am.

22 Q.   And then what was sent to the computer, the computer

23 instructions, you were also given that, correct?

24 A.   We don't have a PCAP file of the instructions being sent.

25 We don't have a --

1 Q. But you actually have the source code that was sent

2 there.

3 A. No, we don't have the source code, we have the computer

4 code, the object code.

5 Q. I'm sorry, the object code. You have that of exactly

6 what was sent there.

7 A. Yes, but that's not -- that's the code that gets to the

8 computer. What's missing is the exploit, and then what's

9 missing is a PCAP file saved from the defendant's computer.

10 Q. And you were also speculating as to looking at a

11 defendant's computer may not be helpful, correct?

12 A. I answered some questions about that.

13 Q. Okay. But you said it would not be helpful.

14 A. I said over time it would be less and less helpful.

15 Q. Okay. But you don't know that for sure, so you're

16 speculating.

17 A. I mean, when you reboot a computer, whatever is in memory

18 disappears. And, so, if you --

19 Q. That's in the ram, not in your hard drive.

20 A. That's correct.

21 Q. And ram is very small in most computers, correct?

22 A. I mean, we generally have much less ram than storage

23 space, yes, ma'am.

24 Q. And most of the things that are found on computers are

25 going to be in your external hard drive, and that, if it's

1 done correctly by a trained forensic person, is going to be

2 the exact same as when that computer was turned off.

3 A.   So the data that the NIT collected, such as the MAC

4 address, that's not stored on the hard drive. That's stored

5 initially in the Wi-Fi card, but it can be changed by running

6 software, and then that would be in memory.

7 Q.   And in this particular case you looked at at least

8 Mr. Eure's information from his computer, correct?

9 A.   I haven't looked at information from his computer, no,

10 ma'am.

11 Q.   Okay. So let's say hypothetically that the MAC address

12 was -- the exact same MAC address that was sent to the FBI

13 was the MAC address of Mr. Eure's computer that contained

14 child pornography.

15   Would that change your speculation as to whether or

16 not you need an exploit to prove any infirmities?

17 A.   No. So, as I said before, having the exploit will give

18 you some indication as to whether the computer was left in

19 either a secure state or an insecure state, and without the

20 exploit you don't know if information that's on the

21 computer -- that's stored on the computer was downloaded by

22 the defendant or may have been put there later by someone

23 else.

24 Q.   How about a defendant -- hypothetically, let's say both

25 defendants, Mr. Eure and Mr. Darby, in this case, confessed

1   that they used Playpen, that they had those exact user names

2   that were in their search warrants, and that they were

3   responsible for what was on their computer and what they saw

4   in Playpen.

5   Would that change your opinion that the exploit and

6   the unique identifier generator is necessary?

7   A.   That they -- so I need to ask a clarifying question of

8   you.

9   Did they say that every single file that was on the

10 computer was downloaded by them?

11 Q.   This is a hypothetical --

12   THE COURT: They didn't say every single file was

13 anything.   They just said the information contained on the

14 computer was their information on their computer.   And the

15 fact that that information was what the FBI had also

16 discovered makes no difference to you, does it?

17   THE WITNESS: If -- knowing -- being able to see the

18 exploit -- and, to be clear, not me but someone skilled in

19 the art of malware and exploit analysis being able to look at

20 the exploit --

21   THE COURT: The question is it doesn't make any

22 difference, because isn't it true that you challenge all

23 computers where they don't use encryption; that is, that

24 includes all e-mail providers, social networking sites, and

25 any Web sites that transmit computer data.   Is that correct?

1   THE WITNESS: I'm sorry, sir, I don't understand the

2   question. Can you ask it again?

3   THE COURT: Let me say this:

4   You challenge all of the companies that are not

5   using an encryption by default. Isn't that correct?

6   THE WITNESS: I have spent several years pushing

7   companies and government agencies to encrypt their data, yes,

8   sir.

9   THE COURT: I didn't ask you about several years, I

10   asked you is it true -- and I'll repeat it -- "I challenge

11   all the companies that are not using https by default."

12   Is that correct?

13   THE WITNESS: Challenge to what? What are you

14   reading from?

15   THE COURT: "...includes all e-mail providers,

16   social networking sites, and any Web site that transmits

17   consumer data. Step up and protect consumers. Don't do it

18   just some of the time, make your Web sites secure by

19   default."

20   THE WITNESS: Okay, now I know what you're quoting.

21   That's a statement by Pamela Jones Harper, a Commissioner at

22   the Federal Trade Commission. Those are not my words, those

23   are hers.

24   THE COURT: So you don't agree with it.

25   THE WITNESS: I agree with it.

1   THE COURT: You printed it.

2   THE WITNESS: I think I cited it.

3   THE COURT: Yes, and you gave it verbatim in your

4   declaration, did you not?

5   THE WITNESS: Sir, that's a quote in a footnote.

6   THE COURT: I understand.

7   THE WITNESS: Okay.

8   THE COURT: But you gave it. I didn't dream it out

9   of the air, did I?

10   THE WITNESS: You didn't dream it out of the air,

11 but --

12   THE COURT: Okay. You know, you're going to have to

13 start answering questions and stop arguing all the time about

14 every question. Nobody is trying to trick you in any way,

15 we're just trying to get at what you're seeking to achieve.

16   You're seeking to achieve the fact that the FBI did

17 not encrypt the material it was sending back, correct?

18   THE WITNESS: Yes, Your Honor.

19   THE COURT: And that's it in a nutshell, isn't it?

20   THE WITNESS: I believe that the government should

21 have encrypted the data, because it would have provided

22 tampered evidence.

23   THE COURT: That's all right. Okay. Let's move

24 along, Ms. Yusi.

25 BY MS. YUSI:

1   Q. Now, you did agree -- just to touch base with the

2   suppression issue, you agree that every user and every person

3   that's been charged, or has allegedly been involved with

4   Playpen and charged, that that person had to choose to go to

5   the Playpen site, correct?

6   A. I don't believe I said that.

7   Q. You said everyone that got the NIT had to go to the

8   Playpen Web site.

9   A. Right, but I didn't say that they had to choose to go.

10 So it's possible to visit the site without choosing to go

11 there.

12 Q. Okay. Let's say they open up an account and they've been

13 seen well before the NIT, they continue to use the site; they

14 use it afterwards, too. Okay? Let's say that. They go

15 to -- they're choosing to go to a Web site at that point,

16 correct?

17 A. Sure.

18 Q. And they have to go to the Eastern District of Virginia

19 to get information from that Web site. Do you agree?

20 A. No, they don't go into the Eastern District of Virginia.

21 Q. They cause their computer to go into the Eastern District

22 of Virginia, or the Internet, or whatever --

23 A. When I call my family in New Haven I'm not entering the

24 City of New Haven, I'm sitting in Washington, D.C. making a

25 telephone call. And my voice is turned into digital data,

1 and it goes over a phone line, but I never leave D.C.

2 Q. You also talked about what the FBI knew in terms of

3 activity of each user on the Web site, correct?

4 A. Yes, ma'am.

5 Q. You said you don't know what they knew, if they knew

6 anything. Is that right?

7 A. Well, so, we've seen in several cases the government has

8 described information in affidavits about how many hours

9 individuals spent logged in to the forums, when they created

10 their accounts. So there's certainly some information that

11 was collected and created initially by the server

12 administrators and then further supplemented by the

13 government.

14 Q. And there's activity logs or user reports?

15 A. Yes, ma'am.

16 Q. And, so, the FBI knew what was going on, at least in

17 those cases that you know about?

18 A. The government knew about activity associated with

19 accounts but not with IP addresses.

20 Q. Right. Until there's a NIT, right?

21 A. Until they hacked the computers of the people visiting

22 the site, yes, ma'am.

23   THE COURT: You have seven minutes left, Ms. Yusi.

24   MS. YUSI: Yes, sir. If I can have one moment.

25   (There was a pause in the proceedings.)

1 BY MS. YUSI:

2 Q. One last thing:

3   You said earlier that encryption is a guarantee of

4 safety, correct?

5 A. Did I say that today?

6 Q. Yes.

7 A. When did I say that? Can you read that back?

8 Q. I don't think we need to, but -- okay. So you agree that

9 encryption is not a guarantee?

10 A. That's correct. Encryption -- just like a doctor washing

11 his or her hands before surgery is not a guarantee that

12 you'll come out of surgery in good condition. If they don't

13 wash their hands, you're going to have a really bad time, and

14 encrypting is a contributing element to good cyber security

15 hygiene.

16   MS. YUSI: Thank you. Those are all my questions,

17 Your Honor.

18   THE COURT: Any other questions?

19   MR. GRINDROD: No, Your Honor.

20   THE COURT: Thank you very much, sir. You may step

21 down.

22   Who is your next witness?

23   MR. GRINDROD: Your Honor, there are no further

24 defense witnesses. We would just offer the transcript from

25 proceedings before Judge Morgan in the United States against

Heidi L. Jeffreys, Official Court Reporter

1 Edward Joseph Matish. The parties have reached an agreement

2 that we will submit this transcript for the Court's

3 consideration with respect to the pending motion to suppress

4 in Mr. Eure's case.

5   THE COURT: The entire transcript from Judge

6 Morgan's case you want to admit?

7   MR. GRINDROD: Yes, Your Honor.

8   MS. YUSI: And, Your Honor, I have no objection, but

9 I do want to say I agreed to this not knowing that we were

10 going to rehash the majority of things for the last two

11 hours. But that's fine, if we still need to do that.

12   THE COURT: Well, we'll just keep going, because I'm

13 going to finish tonight. So don't plan on going anywhere.

14   MR. GRINDROD: Yes, sir, Your Honor. If I could

15 submit this for the Court.

16   THE COURT: All right.

17   MR. GRINDROD: It's been marked as Defendant's

18 Exhibit 1.

19   (The exhibit was admitted into evidence.)

20   THE COURT: I've read Judge Morgan's opinion, which

21 is a very interesting opinion, and it differs somewhat from

22 my prior opinion. So where are we going? This is admitted

23 to show what Judge Morgan's opinion is about, and he ruled

24 against your position.

25   MR. GRINDROD: That's correct, Your Honor. We're

1 certainly not submitting it for the same outcome in that

2 case, but we called Agents McFarland and Alfin in that case

3 to testify, and in order to not just duplicate that testimony

4 we thought it would be more efficient to submit their

5 testimony.

6   THE COURT: So all of your testimony is in here.

7   MR. GRINDROD: Yes, sir, that's the full transcript,

8 including argument. But, I mean, I don't think the argument

9 is necessarily relevant to the --

10   THE COURT: Well, that's what this case has been

11 about, was the whole argument instead of the testimony of a

12 witness. And I don't like it if it's not testimony. I tell

13 you, try to stick to testimony from everyone. It's not any

14 one person.

15   Okay. What else have you got, Ms. Yusi?

16   Have you got anything else?

17   MR. GRINDROD: No, Your Honor.

18   THE COURT: All right. All right, Ms. Yusi.

19   MS. YUSI: Your Honor, I'd like to call Special

20 Agent Alfin. And the transcript, that's regarding the motion

21 to suppress. I'm going to be very brief and just kind of

22 address some of the issues that Dr. Soghoian went into with

23 Special Agent Alfin.

24   THE COURT: Well, let's take a break right now.

25 Let's take a 12-minute break by that clock.

1   MS. YUSI: Yes, sir.

2   (A recess was taken.)

3   THE COURT: All right, Ms. Yusi.

4   MS. YUSI: Thank you. Your Honor, we call Special

5   Agent Alfin from the FBI.

6   (The clerk administered the oath.)

7   DANIEL ALFIN, called as a witness, having been first

8   duly sworn, testified as follows:

9   DIRECT EXAMINATION

10   BY MS. YUSI:

11   Q. Could you introduce yourself, Special Agent Alfin, to the

12   Court?

13   A. My name is Daniel Alfin, last name spelled A-L-F-I-N. I

14   am a Special Agent with the FBI. I'm currently assigned to

15   FBI Headquarters, Criminal Investigative Division, Violent

16   Crimes Against Children Section, Major Case Coordination

17   Unit, located in Lithicum, Maryland.

18   Q. And how long have you been an FBI agent?

19   A. I've been employed as an FBI agent since 2009.

20   Q. And in your current position what sort of cases do you

21   work on?

22   A. My role at the Major Case Coordination Unit is to

23   investigate individuals who use various types of technology

24   to facilitate the production, trade, and distribution of

25   child pornography. Specifically, my investigations involve

1 individuals who use the Tor network.

2 Q.   Are you the case agent for the national Playpen

3 investigation?

4 A.   I am.

5 Q.   And when did you start being involved with the

6 investigation of Playpen?

7 A.   I became aware of Playpen shortly after it came online in

8 approximately August, 2014.

9   In December, 2014, the FBI learned the true location

10 of the Playpen Web site, and we initiated an investigation.

11 I have been involved in that investigation from the

12 beginning.

13 Q.   Okay. And you've submitted a declaration in this case

14 and others concerning the NIT that was involved in the

15 investigation?

16 A.   I have.

17 Q.   All right. And I'm going to talk to you just briefly

18 about or ask you questions about certain points. You were

19 here when Dr. Soghoian testified, correct?

20 A.   I was.

21 Q.   All right. He talked about encryption and the

22 possibility of someone tampering with the information that

23 came from the user to the FBI servers. Can you talk about --

24 well, the FBI did not use encryption, correct?

25 A.   That is correct, the information transmitted by the NIT

1   was not encrypted.

2   Referring to Dr. Soghoian's testimony, in theory he

3   is correct. Generally, data that is not sent in an encrypted

4   format can be tampered with. That is a theoretical

5   possibility; however, it is not an issue in the matter at

6   hand for a number of reasons. Despite the fact that the data

7   that we sent was unencrypted, a number of things would have

8   had to have taken place in order for someone to tamper with

9   it.

10   First of all, an individual would have had to have

11   known about the FBI's operation. They would have had to have

12   known sensitive government information about the FBI takeover

13   of a Playpen Web site. They would have had to have known

14   that we were deploying a NIT on the Web site to identify

15   users. They would have had to have known how the NIT

16   functioned and how it sent data back to the FBI.

17   Additionally, a user would have had to have known

18   information from the defendant's computer. They would have

19   had to have known the unique identifier on the defendant's

20   computer, previously referred to as a MAC address, among

21   other pieces of information. They would have had to have

22   known that the defendant was a member of the Playpen Web

23   site.

24   In addition to all of this, an attacker would have

25   had to have the capability to intercept the data from the

---
D. Alfin - Direct
---

1 defendant's computer to the government. There is no person

2 or organization that could have known or had the capability

3 to do all of these things, and so I can say with certainty

4 that the data that was collected by the government in this

5 operation is true and accurate.

6 Q. Now, I'd like to talk to you about what has been made

7 available to the defendant.

8   Could you describe the two things that have been made

9 available to the defendant?

10 A. A number of things have been made available to the

11 defendant. All of these things are the necessary pieces of

12 information that would be needed to prove what has been

13 referred to as a digital chain of custody.

14   First of all, we have made available to defense for

15 review the NIT that seized the data from the defendant's

16 computer. We have also made available to defense the

17 defendant's computer itself from which that data was seized.

18   Additionally, we have made available to defense the

19 network data that was captured by the government, showing the

20 data that the NIT sent to the government from the defendant's

21 computer.

22   These three things on their own can prove the

23 digital chain of custody, showing that the data originating

24 from the defendant's computer was, in fact, what was

25 collected by the government and what was, in fact, used in

1   its investigation of the defendants.

2   A fourth piece of information that further

3   emphasizes the fact that the data collected was accurate is

4   the fact that the defendants admitted to the activity on the

5   Playpen Web site of which they were accused. The primary

6   purpose of the NIT was to associate a user account on Playpen

7   with a real-world person. In both instances at hand both

8   defendants admitted to that activity, so that further throws

9   out any concern of alleged digital chain of custody issues.

10   Q. Do you know if either of the defendants have requested

11   that a forensic person or someone else, another expert, look

12   at the computers that were seized from their house?

13   A. It is my understanding that the digital devices seized

14   from the residences of the defendants have been made

15   available to defense for review; however, defense has not

16   made any attempts to review or analyze those devices.

17   Q. Now, in order to also, I guess, test your theory -- or

18   not your theory but what the FBI said, the information that

19   matches the computer back to what the FBI received, did you

20   do any tests, or are there any tests available to do that?

21   A. Yes. In order to validate that the information that the

22   government received and provided the defense is accurate, you

23   would need to analyze a number of pieces of information, all

24   of which I described previously, all of which are available

25   for defense to review, including the defendants' computers,

1 the network data stream, the actual NIT, and the statements

2 made by the defendants.

3 Q. And with that information can they -- what can they do

4 with it in a sterile environment, I guess, to test it?

5 A. All that information that has been provided to defense

6 can be used to confirm that the evidence used in the charges

7 at hand were -- that that evidence was good and accurate.

8   Additionally, the NIT source code that has been

9 provided to defense can confirm that the information that the

10 NIT was authorized to collect is the same as the information

11 that the NIT did, in fact, collect and that it did not

12 collect anything outside the scope of the warrants that

13 authorized its use.

14 Q. Dr. Soghoian also talked about "unique identifier

15 generator." Did you hear that testimony?

16 A. I did.

17 Q. And can you expound on what he said?

18 A. When the NIT is downloaded to a user's computer it

19 includes a unique identifier. Every identifier generated

20 during this operation was, in fact, unique. I know this

21 because as the case agent I have access to every single

22 unique identifier that was generated in this investigation.

23   I have reviewed every single unique identifier in

24 this investigation in order to determine that there were, in

25 fact, no unique identifiers generated more than once.

1   Q. If you had found a duplicate unique identifier, what

2   would you have done with that information?

3   A. If a unique duplicate identifier had been found, I would

4   have attempted to identify the source of that duplication;

5   however, there were no unique identifiers generated, so it's

6   not an issue that I had to deal with.

7   Q. Okay.

8   MS. YUSI: Your Honor, I think those are all of my

9   questions at this time.

10   THE COURT: Mr. Grindrod.

11   MR. GRINDROD: Thank you, Your Honor.

12   CROSS-EXAMINATION

13   BY MR. GRINDROD:

14   Q. Let's pick up where Ms. Yusi left off. You were talking

15   about the unique identifier or the creation of unique

16   identifiers.

17   A. Yes.

18   Q. And you talked about a list of unique identifiers that

19   you reviewed.

20   A. Yes.

21   Q. Was that the list of the unique identifiers that were

22   sent out by the FBI or the list of unique identifiers that

23   were successfully returned to the FBI?

24   A. It was the list of unique identifiers that were generated

25   by the FBI. So "sent out by the FBI," I think that would be

1   an accurate description.

2   Q. And you reviewed that list and compared, what, each

3   unique identifier to every other identifier?

4   A. It's a very simple process. You put every unique

5   identifier in a spreadsheet, and you say "find duplicates"

6   and the spreadsheet says there are no duplicates. It's very

7   simple to do.

8   Q. Have you produced that spreadsheet to the defense?

9   A. No. I have provided the unique identifier used in the

10 matter at hand.

11 Q. And even if you're not providing the code that created

12 the unique identifier, to your knowledge, has the government

13 produced any indication as to how that unique identifier was

14 even created?

15 A. Yes, we generated unique identifiers.

16 Q. Using an algorithm?

17 A. Yes.

18 Q. Did you write that algorithm?

19 A. I did not.

20 Q. Do you know that algorithm?

21 A. I do not.

22 Q. Would you recognize it if you were presented with it?

23 A. I would not.

24 Q. Can you explain the inner workings of how that algorithm

25 works?

1   A. I can. It generates a unique identifier.

2   Q. That's the inner workings, as far as your understanding

3   goes?

4   A. Could you be more specific in what you're asking for?

5   Q. Well, this unique identifier is a piece of computer code,

6   correct?

7   A. No, it's a string of text.

8   Q. It's a string of text?

9   A. A unique identifier is a string of text, yes.

10   Q. It's a generator. It's computer code.

11   A. The generator could be described as computer code, yes.

12   Q. And it runs on a system.

13   A. Yes.

14   Q. What system does it run on?

15   A. A government-controlled computer.

16   Q. Okay. And is it operated inside any -- is it just

17   operating in some program that is unique that is created by

18   the government in order to create these unique identifiers?

19   Does it run within Excel? You mentioned that there may be

20   spreadsheets involved.

21   I'm trying to figure out how, from a technological

22   perspective, this generator worked.

23   A. When a NIT is packaged or put together it generates a

24   unique identifier, and it injects it into the package that is

25   downloaded to the user's computer.

1   Q.   Okay. And that's what it does, but now my question is

2   how does it do that?

3   So this creation of a unique identifier, you said

4   that that is created through some sort of computer code.

5   What I'm trying to figure out is how exactly, from a

6   technological perspective, is the unique identifier created?

7   MS. YUSI: Your Honor, I'm going to object.

8   THE COURT: We're going into the code itself. Isn't

9   that where we're going?

10   MR. GRINDROD: Your Honor, in the event the

11 government is not going to produce it, perhaps Agent Alfin

12 can explain how the code works so that we can understand why

13 there is some alleged law enforcement privilege that covers

14 it.

15   MS. YUSI: Your Honor, if I may interject, I don't

16 think any of these other unique identifiers are important.

17 The only ones that are important are the ones that went to

18 the two defendants.

19   THE COURT: Well, there isn't any question the --

20 there is testimony that an IP, I believe, was different from

21 one sent that one existed, and I thought we would probably be

22 going into that some day.

23   MS. YUSI: That's a separate issue, Your Honor.

24   THE COURT: Well, I'm not going into the code. I

25 can tell you that. And we're not going into the code, so --

1   at this time. We may go into the code later, but it's only

2   after I make a ruling on whether the code is discoverable or

3   not. So we're not going into it at this time. We're knowing

4   that the code was utilized, and that's all that I'm going

5   into or all I'm going to allow at this particular portion.

6   So let's don't go into what the code is or does and how it

7   works, because that's one way that it could be released. The

8   problem about codes that invade Tor is what it may lead to.

9   We have tremendous security problems at the present

10   time with encrypted materials being utilized by those people

11   whose main object in the makeup of things at the present time

12   is to kill nonbelievers, and unfortunately there are a great

13   many nonbelievers right in this room at this time. And so,

14   therefore, they are everywhere. And since there is an

15   organization who would love to get into Tor to find out what

16   the government is doing, I'm not about to release anything

17   unless it's essential, and then the government would have to

18   decide whether it's going forward or not with the case.

19   MR. GRINDROD: I understand, Your Honor.

20   THE COURT: But I'm not going to go into it on

21   examination of this witness.

22   BY MR. GRINDROD:

23   Q. Agent Alfin, without providing any further explanation

24   than what you've already provided, can you just tell me

25   whether you have -- you personally could give any more

1   detailed explanation about how the code worked than what

2   you've already provided here in court?

3   A.   Which specific code?

4   Q.   The unique identifier generator. Just a "yes" or "no."

5   I don't want to get into any --

6   THE COURT: Unique identifier -- which one are you

7   speaking of, the one that found Tor or the one that found the

8   defendant?

9   MR. GRINDROD: I think Your Honor may be referring

10 to the IP address.

11   THE COURT: Yes.

12   MR. GRINDROD: And I'm referring, instead, to the

13 FBI-generated code that was injected into the packet of

14 information that was sent from our clients' computers to the

15 FBI as a means of linking up the Playpen use with the user

16 account. This was a number that the FBI created in order to

17 uniquely identify people, and what I'm trying to figure out

18 is whether Agent Alfin even has an understanding as to how

19 that code worked.

20   THE COURT: I'll allow that.

21 BY MR. GRINDROD:

22 Q.   So, Agent Alfin, I'll ask you again. Again, without

23 providing a substantive answer as to how the code may or may

24 not have worked, do you have the ability to provide any more

25 detail as to how the unique identifier generator worked in

1 this case from a technological perspective?

2 A. I've already explained in detail how it works from a

3 technological perspective, so I would still need you to

4 clarify what exactly you're asking, because your questions

5 don't make sense from a technical standpoint.

6 Q. So, as far as you're concerned, everything about how it

7 works has been said.

8   THE COURT: I don't know about everything, but --

9   THE WITNESS: I have not --

10   THE COURT: Where has it been said?

11   THE WITNESS: The actual mathematical algorithm that

12 generates the unique identifiers, that has not been stated.

13 I do not know that mathematical algorithm.

14 BY MR. GRINDROD:

15 Q. Or how it was created?

16 A. How the mathematical algorithm was created?

17 Q. What went into its design? Presumably, the point of the

18 algorithm is to ensure it produces unique numbers.

19   THE COURT: I'm not going into how --

20   MR. GRINDROD: I'll move on, Your Honor.

21   THE COURT: -- it was created, because that will

22 imply a knowledge of how to get it.

23   MR. GRINDROD: I'll move on, Your Honor.

24   THE COURT: I'm not going to get into that, unless I

25 find that the motion to produce or the motion to compel or

———— D. Alfin - Cross ————

1   the motion to suppress is merited. First I'd have to find

2   that, and then you can go into it, but you're not going into

3   it indirectly, okay?

4   MR. GRINDROD: Understood, Your Honor.

5   BY MR. GRINDROD:

6   Q. Agent Alfin, you've obviously prepared a declaration in

7   this case and now testified, so I want to talk a little bit

8   about your credentials.

9   Your declaration states that you hold a university

10 degree in information technology. Can you tell me what

11 that's in reference to?

12 A. I have a Bachelor's degree in information technology.

13 Q. And where is that from?

14 A. Florida State University.

15 Q. And did your training in information technology include

16 computer science courses?

17 A. Yes.

18 Q. And do you have a working ability to write computer code?

19 A. Basic computer code, yes.

20 Q. But it's fair to say you're not capable of writing, for

21 example, the NIT in this case.

22 A. The NIT is actually very simple computer code.

23 Q. Did you help write it?

24 A. I did not.

25 Q. Could you write a NIT?

D. Alfin - Cross

1   A.   The NIT that was used in this case? Yes, I do have the

2   capabilities to write a NIT similar to this one.

3   Q.   Okay. And the NIT was produced in this case, right?

4   A.   It was.

5   Q.   Let's talk about the exploit, then.

6   Do you have the technical capability to write an

7   exploit?

8   A.   I do not.

9   Q.   Did you work at all in the creation of the exploit in

10 this case?

11 A.   I did not.

12 Q.   You've obviously testified, both here and in your

13 declaration, about what the exploit does and doesn't do,

14 correct?

15 A.   Yes, I have.

16 Q.   Is that based on your review of the exploit?

17 A.   It is based on my use of the exploit.

18 Q.   Okay. And you make that clarification because you've

19 never actually reviewed the exploit, correct?

20 A.   Are you referring to the source code of the exploit?

21 Q.   Well, have you looked at the source code of the exploit?

22 A.   I have not.

23 Q.   Have you looked at any other aspect of the exploit?

24 A.   Such as...

25 Q.   Such as -- so the --

1   THE COURT: The exploit is the code.

2   MR. GRINDROD: Well, that's where it gets tricky,

3   Your Honor. I think there are various things that can be

4   referred to as "the code" in this case, but the exploit is a

5   code, that's correct.

6   So the source code --

7   THE COURT: What was the exploit in this case, I

8   understood, was the code utilized in this case. So there's

9   another exploit besides the code that was used in this case?

10   MR. GRINDROD: Well, Your Honor, "an exploit" can

11   describe --

12   THE COURT: I know what an exploit is in this case;

13   it's the code utilized in this case.

14   MR. GRINDROD: Correct.

15   THE COURT: And that's what's referred to in various

16   declarations and in various testimony. Now we've got a

17   different exploit?

18   MR. GRINDROD: No, Your Honor, but there are

19   different -- so the NIT computer code is sometimes referred

20   to as a code. That's a separate thing.

21   THE COURT: I understand the NIT is one thing.

22   MR. GRINDROD: Right.

23   THE COURT: The exploit was the code utilized to

24   determine the defendant's computer, correct?

25   MR. GRINDROD: To determine -- no -- well, I don't

1 think so, Your Honor. I think the exploit was what was used

2 to hack into our client's computer. The NIT is what was used

3 to actually collect the data and send it back to the FBI.

4   I think Dr. Soghoian referred to the exploit as the

5 picking of the lock or the exploit as the drugged piece of

6 meat that the guard dogs eat. It's what let the government

7 into our clients' computers.

8   THE COURT: All right. Let's go ahead. We've got

9 to get into it some day.

10 BY MR. GRINDROD:

11 Q. So you've not reviewed the exploit in this case. Is that

12 correct?

13 A. I have not reviewed the exploit source code in this case.

14 Q. And all of the statements you're making about what the

15 exploit does and doesn't do, those statements are based on

16 your observations of running the exploit. Is that correct?

17 A. In part, yes.

18 Q. What else are they based on?

19 A. Based on my conversations with other people who are

20 knowledgeable in the matter, as stated in my declaration.

21 Q. Who are those people?

22 A. Other FBI personnel.

23 Q. Yeah, but what people?

24 A. That information is subject to law enforcement privilege.

25 Q. The names of the people who -- so you're basing your

1   testimony on what you were told by other individuals, at

2   least in part.

3   THE COURT: In part, okay?

4   BY MR. GRINDROD:

5   Q. Is that correct?

6   A. Everything substantive in my declaration is based on my

7   own observations of my own testing. It has been further

8   supported and backed up by other statements I've received

9   from other individuals; however, I have tested everything

10   with regard to the NIT's functions in my declaration.

11   Q. Okay. So help me understand the process. So you run the

12   exploit, you make certain observations, and you draft this

13   declaration. Is that what happened?

14   A. That's fair. That is an accurate order of events.

15   Q. And then at that point, after you drafted the

16   declaration, you went to other folks in the FBI and said,

17   "Does this look right to you?"

18   A. No, that's not what I said.

19   Q. Okay. So tell me how -- what part of this declaration --

20   A. There are other individuals at the FBI who obviously have

21   reviewed the source code of the exploit. I have had

22   conversations with those individuals --

23   Q. And the conversations --

24   A. -- several times throughout the course of this

25   investigation, both before and after I wrote my declaration.

1 Q. So it's fair to say there are people who are more heavily

2 involved in the tech side of this than you, correct?

3 A. In certain aspects of it, yes, that's true.

4 Q. Specifically with regard to the exploit, right?

5 A. Yes, that's true.

6 Q. Because you don't have the ability to create the exploit.

7   THE COURT: He's already testified to that three

8 times now. Don't ask it again, please. Let's move on.

9 BY MR. GRINDROD:

10 Q. And, so, is there any way that you can be more specific

11 as to what parts of this declaration that you submitted to

12 the Court is based on your own personal observations versus

13 your conversations with other people?

14 A. I think I've been clear on that, but if you have

15 questions about a specific portion of my declaration, I'd be

16 happy to answer.

17 Q. Okay. So let's be specific about paragraph 14. So in

18 paragraph 14 the first sentence says, "It's theoretically

19 possible for an exploit to make fundamental changes or

20 alterations to a computer system or to disable its security

21 firewall."

22   Is that based on your own personal knowledge?

23 A. Yes, it is.

24 Q. So it's possible for an exploit to make fundamental

25 changes or alterations to a computer.

––––––––D. Alfin - Cross––––––––

1 A. An exploit. Not the one in this case, but yes.

2 Q. Okay. So let's figure out what the source is for that

3 part of your statement.

4   The part of your statement in which you say this

5 exploit specifically didn't make fundamental changes, is that

6 based on your personal observations or based on what other

7 FBI agents have told you?

8 A. I tested a NIT on a computer -- or, rather, the exploit

9 on a computer under my control. I observed that it did not

10 open up any security holes on it, it didn't place any files

11 on it, it didn't make it any more vulnerable to outside

12 attackers. It is based on my observations and my testing.

13 Q. And how many times did you run the exploit before you

14 reached that conclusion?

15 A. A few times. I don't know the exact number.

16 Q. More than five?

17 A. Possibly. Less than a hundred.

18 Q. Was it less than ten?

19 A. It may have been.

20 Q. Okay. Have you received any training on how to test

21 software or computer code like an exploit?

22 A. I have.

23 Q. And where was that training?

24 A. I have received courses in malware analysis put on by FBI

25 and FBI contractors.

1   More importantly, I have conducted analysis of such

2   code on several occasions during the course of both criminal

3   investigations and national security investigations. I have

4   analyzed exploits used by criminals trying to steal money. I

5   have analyzed exploits used by foreign countries trying to

6   steal state secrets.

7   In all of these cases I have successfully found and

8   analyzed this code without -- obviously, these foreign

9   governments were not kind enough to give me the exploit on

10 the front end; however, that did not stop me from being

11 successful in my analyses.

12 Q.   And as part of that training that you received were you

13 taught the appropriate way to test an exploit to determine

14 whether it creates software vulnerabilities is to run it been

15 5 and 10 times?

16 A.   You can run an exploit that does one thing as many times

17 as you want. If it's programmed to do one thing, it's going

18 to keep doing that one thing.

19 Q.   Okay. So my question was did you receive as part of --

20 you said you received training in malware analysis, and I'm

21 asking whether as part of that training you were taught that

22 an appropriate means of testing an exploit to determine

23 whether it makes fundamental changes or alterations to a

24 computer system is to run that exploit between 5 and 10

25 times.

1   A.   I don't recall whether or not there was a number involved

2   in that training.   I was taught how to analyze malware.

3   Q.   So you don't have any recollection --

4   THE COURT: He wasn't taught in that training.

5   Don't argue with the witness.   Let's go along and ask

6   questions.

7   BY MR. GRINDROD:

8   Q.   Was the NIT ever programmed to collect the IP address of

9   the activating computer?

10 A.   The NIT collects pieces of information identified in the

11 NIT search warrant attachment and transmits it to the

12 government.   At that point we can see the IP address that

13 data is originating from.

14 Q.   Let me ask you my question again.

15   Was the NIT ever programmed to collect the IP address

16 of the activating computer?

17   THE COURT: Of whose computer?

18   MR. GRINDROD: The activating computer, the user's

19 computer.

20   THE COURT: The user's computer.   Go ahead.

21   THE WITNESS: Your question is not technically

22 sufficient for me to answer it "yes" or "no," and so I would

23 have to rely on my statements, unless you can rephrase your

24 question.

25 BY MR. GRINDROD:

1 Q. Do various forms of the NIT exist?

2 A. Yes. Or, rather, multiple -- every NIT used in this case

3 was unique.

4 Q. And were there ever versions of the NIT that was used in

5 this case that instead of collecting the IP address as sort

6 of a byproduct of the other information -- was the NIT ever

7 written in a way so that it collected the IP address from the

8 activating computer itself?

9 A. Could you define what you mean by "collect" in that

10 statement?

11   THE COURT: From which computer are we speaking of,

12 now? You've got two computers that I think we're interested

13 in. One is the computer that was transmitting Playpen, and

14 the other was the computer utilized by the defendants or one

15 or more of the defendants.

16   So we have actually three computers involved in the

17 motion to compel, as I understand it. We may have four,

18 because there may have been another computer transmitting

19 information, as the other expert has testified to, a

20 different computer transmitting the information back to the

21 FBI than there was collecting information. So there may be

22 four computers.

23   MR. GRINDROD: I'll try to be more specific as to

24 the computer.

25   THE COURT: All right.

—————— D. Alfin - Cross ——————

1   BY MR. GRINDROD:

2   Q. So, Agent Alfin, when I use the term "activating

3   computer" or "the user's computer" I'm talking about the

4   defendant's -- the to-be-defendant's computer, the computer

5   that was the target of this search. Do you understand that?

6   A. Yes.

7   Q. Okay. So my question was whether the NIT -- whether

8   there was ever any version of the NIT that gathered from the

9   operating system the IP address of that activating computer.

10 A. I still need you to be more specific. When you say

11 "gathered" do you mean sent back to the government?

12 Q. No, I mean gathered.

13 A. If it wasn't sent to the government, it wasn't gathered.

14 Q. Okay. Well, what word can I use to --

15 A. Well, let me rephrase. Who is gathering it, then?

16 Q. The FBI, through the NIT.

17 A. So it is sent to the FBI in your question.

18 Q. I'm not concerned really -- so let me break it down.

19   So the NIT you can think of as having two stages,

20 right? Part of what the NIT does is once it gets onto our

21 client's computer, onto the activating computer, it gathers

22 certain information, right -- the MAC address, the host

23 name -- gathers that information and then packages that

24 information and sends it -- as part two, it sends that

25 information that it gathered to the FBI server, correct?

1 A.   That's accurate.

2 Q.   Okay. So I'm not concerned for the purposes of this

3 question with what was sent to the FBI. I want you to focus

4 for purposes of this question on what information was

5 gathered to be packaged on the activating computer.

6   THE COURT: If it wasn't sent to the FBI, how would

7 he know what was packaged?

8   MR. GRINDROD: Well, Your Honor, I think he's going

9 to testify that --

10   THE COURT: All right.

11   THE WITNESS: I'm familiar with Dr. Soghoian's

12 testimony, and I know where you're going with this, so if you

13 will just allow me to testify I think I can put the issue to

14 rest, if that satisfies.

15 BY MR. GRINDROD:

16 Q.   Well, are you capable of answering the question?

17 A.   Yes, I am capable of answering the question.

18 Q.   Okay. Can you answer the question?

19 A.   The NIT that you're referring to -- I just want to

20 clarify. Is it the one that was used in the matter at hand?

21 Q.   Yes.

22 A.   Okay. So in some instances, for some of the NITs, in

23 order to collect certain pieces of information such as the

24 MAC address the NIT executes a command that displays the MAC

25 address. It also displays, in some cases, the local IP

1   address of the computer, which is also covered by the NIT

2   search warrant. However, that information is not relevant or

3   important to the FBI. It is not parsed out, and it is not

4   sent to the FBI.

5   So, to answer your question, the NIT itself does not

6   gather an IP address. It does not gather an IP address from

7   the computer. I think you're discussing a semantic argument,

8   but it does not gather it, because that implies that we

9   collected it and received it.

10 Q. Okay. I don't know what the right word is -- "gather"

11 obviously isn't it -- but I'm trying to get you to focus on

12 not what was sent to the FBI but what your NIT, the FBI NIT,

13 was designed to collect for packaging.

14   THE COURT: What information is the NIT designed to

15 obtain?

16   THE WITNESS: Several pieces of information, Your

17 Honor, but the most important one, the one that identifies

18 the defendant, is his IP address, the one that's assigned to

19 him from his Internet service provider. And, so, when the

20 NIT communicates back to the FBI we can see which IP address

21 that communication is coming from.

22 BY MR. GRINDROD:

23 Q. So is it correct that, in fact, at least some versions of

24 the NIT collect, not as in transmitting back to the FBI but

25 packaging --

1   THE COURT: When you use the word "collect" or

2 anything else we're using what information was derived.

3   Now you want to -- if they -- I assume that we're

4 worried about the words "collect" and "gather," so why don't

5 we use, "What did you learn from this," "What did you expect

6 to learn from it." I don't mind any of this, other than the

7 fact that we're having a dispute as to the terminology of the

8 utilization of words in this case.

9   And if we can move it along -- that's why I asked

10 what information did they collect -- did they obtain, I

11 should say, not "collect."

12   MR. GRINDROD: I'll try, Your Honor. The problem --

13   THE COURT: I don't know where we're going with it.

14 Are you trying to find out what information was on the

15 computer that they did not use?

16   MR. GRINDROD: Your Honor, I don't know what Agent

17 Alfin will testify to, but I suspect that -- there's reason

18 to believe that the NIT gathered certain information from our

19 clients' computers without transmitting that information back

20 to the FBI and instead deleted or blocked certain aspects of

21 that code from transmitting data and instead transmitted

22 other data through this --

23   THE COURT: What you're saying, in essence, is you

24 have some information that the FBI has transmitted false

25 information back and claimed it was your defendants'

1   information. Isn't that correct?

2   MR. GRINDROD: I'm not sure I can make that

3   representation, no, Your Honor.

4   THE COURT: Well, somewhere or another you're going

5   to have to have some evidence of some kind to go into this.

6   We're all in suppositions, and suppositions are wonderful.

7   In fact, I suppose I'd like to go to the moon, but I don't

8   know if I'm going to get there or live that long. But some

9   people may get there; I'm not sure who. Right now I don't

10   know, but it is possible. Do you understand?

11   So we're not interested in possibilities, we're

12   interested in, you know, what has happened in this case --

13   MR. GRINDROD: That's correct.

14   THE COURT: -- and what the FBI did or did not do.

15   Now, I understand nothing was encrypted in this

16   case, so consequently the question then is how reliable is

17   it? It appears to me that it may be a jury question as to

18   how reliable something may be, but it is not a legal question

19   of how reliable it is.

20   MR. GRINDROD: That's true, Your Honor.

21   THE COURT: So the question really boils down to a

22   question of fact for a jury to determine, unless there is

23   some evidence which would place it in a position where the

24   motion should be granted or not granted here. And so far all

25   I've heard is some suppositions about what's possible on the

1   computer or what can or may be done with computers that are

2   not encrypted.

3   In fact, I'm not so sure that encryption does much

4   good when I realize how much is stolen from banks over a

5   computer system that's totally encrypted. And I'm only

6   relying on news broadcasts for that; I don't know. I haven't

7   had a case on the stealing from banks by computers.

8   So the case which we're interested in is was there

9   an unreasonable search in this case resulting in the

10   obtaining of evidence illegally, not a question of whether

11   they legally obtained evidence, so I want to get to that, if

12   I can. And we've been here a couple of hours dealing in the

13   possibilities of various things, and I don't mind going into

14   it, but some of it is farfetched.

15   MR. GRINDROD: Your Honor is exactly right. I think

16   a lot of these things are questions for the jury.

17   The reason I'm offering this testimony and a lot of

18   the testimony from Dr. Soghoian was to make clear that there

19   are substantial factual questions, and those questions --

20   THE COURT: There are always factual questions in

21   that regard. There may be a very simple answer to a lot of

22   simple questions. I'm not in any way suggesting that it's

23   substantial or insubstantial.

24   MR. GRINDROD: Fair enough, Your Honor.

25   THE COURT: I make sure that there's no ruling of

1   mine which indicates that possibilities are substantial or

2   insubstantial. Possibilities can grow into more than just

3   possibilities, they can become probabilities, which is a

4   situation that is more than 50 percent of the time.

5   MR. GRINDROD: I only mean to say, Your Honor, these

6   questions are aimed at our motion to compel, and so that's

7   why some of these may seem like trial issues.

8   THE COURT: In relation to the motion to compel,

9   there must be some evidence, one, that either the FBI was

10   dishonest or that they wrongly used some search warrant or

11   that the search warrant -- well, in the motion to -- it's not

12   the motion to suppress that deals with the search warrant,

13   we're talking about the motion to compel the disclosure of

14   the code, and I'm not about to disclose the code unless I

15   find that it is material to the defense in this case.

16   So far I don't know what it is that's been testified

17   to as to the materiality of the code in this case. The

18   question of its materiality has to do with the guilt or

19   innocence of the defendants, and that has to do with did the

20   defendants in this case utilize and receive pornographic

21   material in relation to children, and what the type of the

22   particular material was that it may or may not have received.

23   So far I haven't heard any evidence on materiality in

24   relation to the code. The code merely gave the FBI the means

25   to find the particular Internet company that was delivering

1   material as well as the particular Internet company that

2   received the material. And the question in this case is in

3   discovery it deals with materiality, and we're dealing in a

4   lot of suppositions, Mr. Grindrod.

5   I'm not trying to chide you or disturb you. There's

6   no question in my mind that the Internet is possible for

7   hackers to do most everything with the Internet. They can

8   even claim to hack the Secretary of State's Internet. Now we

9   know that there's going to be no prosecution of the Secretary

10   of State, so we can talk about it.

11   But the question is we know that that can be hacked.

12   What is it that we don't know? What we don't know only is

13   what is that code and how valuable is that code, and what

14   could we sell it for, and what could we achieve with it.

15   I imagine people would pay millions to get that

16   code, enough so that the government wouldn't prosecute some

17   people if I ordered it produced, and they may not prosecute

18   these two if I ordered it produced. But that's only if I

19   find that the material is such as to affect the outcome of

20   this case in some fashion, and I haven't seen it yet.

21   MR. GRINDROD: I understand, Your Honor. I'll try

22   to --

23   THE COURT: I'm not trying to stop you.

24   MR. GRINDROD: Okay.

25   THE COURT: You've got the fact that, number one,

1 the testimony of the expert is clear. There's no question

2 that there's no protection for that which is transmitted on

3 the Internet. Whatever you transmit on the Internet,

4 somebody can receive it. If it's encrypted, then a clever

5 hacker who can understand how to encrypt things can find it.

6 In fact, the FBI was particularly adept at hacking itself.

7 It hacked into Tor, whether anybody believes it or not. So

8 they hacked in, and they found it, and the question is what

9 did they find? They found a place that transmits child

10 pornography.

11   I don't know where we're going with child

12 pornography, but it's a very basic thing that we should try

13 to eliminate, if possible; that is, the utilization of

14 children in these matters. In almost every case that I have

15 seen the children of the individuals who utilized them to

16 make these pictures end up with huge problems later on in

17 life -- huge. Or evidently they do. Almost every

18 psychiatrist indicates the same. So the question is whether

19 we can stop the utilization of these children.

20   MR. GRINDROD: Well, I --

21   THE COURT: The question before me today is

22 materiality. You know that, I know that.

23   MR. GRINDROD: And I only have two more quick lines

24 of questioning on those points, Your Honor.

25   THE COURT: I'm not trying to stop you, I'm trying

1 to define what I'm interested in hearing; not learning about

2 the computer as much as I am about what is material that may

3 help the defendant's case as a matter of probabilities, not

4 possibilities, okay?

5   MR. GRINDROD: Yes, sir.

6 BY MR. GRINDROD:

7 Q. Agent Alfin, how many computers did the NIT deploy

8 against?

9 A. In the matter at hand for two defendants? Two computers.

10 Q. For the Playpen operation as a whole, for all users of

11 the Playpen site.

12 A. There were a number of other defendants who were not

13 charged in the matter at hand. The total number of users

14 that were identified by the FBI is known to me. I would ask

15 the Court's permission not to answer that question, because

16 it could give other individuals insight into the full scope

17 of the FBI's operation.

18   Specifically, we identified a number of people in

19 foreign countries, and some foreign countries are very slow

20 to act on the information that they receive because it has to

21 go through official diplomatic channels. More importantly,

22 it's not relevant to the matter at hand. In the matter at

23 hand there are two defendants. We deployed the NIT against

24 two computers. Both of those computers are available to the

25 defense. It has no bearing on these defendants how many

1   other people were identified in the case.

2   THE COURT: But many people were identified,

3   correct?

4   THE WITNESS: Yes, Your Honor.

5   MR. GRINDROD: Your Honor, I do think, especially

6   with respect to the particularity argument on our pending

7   motion to suppress, it is relevant. I'm not sure that the

8   legal argument from Agent Alfin is --

9   THE COURT: I don't know that -- my view is that

10   what they're saying is that it's unique to the proper...

11   (There was a pause in the proceedings.)

12   THE COURT: I'm going to sustain the objection made

13   by the witness.

14   BY MR. GRINDROD:

15   Q. Is the NIT classified?

16   A. The NIT is not classified.

17   Q. Is the exploit?

18   A. At the moment I believe that it is undergoing review;

19   however, further information about that is answered in the

20   declaration that I believe is under seal.

21   Q. You testified in a case called United States v. Michaud.

22   Is that correct?

23   A. I did.

24   Q. Was the exploit -- well, first of all, was it classified

25   at that time?

1   A.   The actual exploit at that time? I do not believe it was

2   classified.

3   Q.   Was it undergoing review, as you say it is now?

4   A.   I don't know exactly when that review process began. I'm

5   not involved in it.

6   Q.   When did you learn about it?

7   A.   At some point in the past year.

8   Q.   Can you be any more specific?

9   A.   No. Again, the government's position is that the exploit

10 is not material to the case at hand. I don't recall that

11 particular conversation.

12   However, I did learn in the past year that it is

13 undergoing --

14   THE COURT: Well, he asked you if it was very

15 material in this case, but the question of determining the

16 exploit, which is the code, I'm not allowing at this time.

17   MR. GRINDROD: Understood, Your Honor.

18 BY MR. GRINDROD:

19 Q.   Was the exploit in this case transmitted to everyone

20 against whom the NIT was deployed?

21   THE COURT: It wasn't transmitted to anyone, as far

22 as I know. Has the exploit itself, the code, been

23 transmitted to anyone, or --

24   THE WITNESS: Your Honor, if I can clarify some

25 earlier points, there are two important pieces of computer

1 software. The first one is the exploit, and that can be

2 thought of as an open window. So we want to seize

3 information from the defendant's computer, and so there's a

4 vulnerability, an open window, on the defendant's computer.

5 We know about it, and that's how we're able to retrieve

6 information from his computer. So we go in through that open

7 window, the exploit, and then the NIT is the code that we've

8 turned over. That is what seizes the information and sends

9 it back to the government.

10   So the exploit, the open window, is the part that we

11 have asserted law enforcement privilege. The NIT, the part

12 that actually seizes the data that actually collects

13 information that was used to identify the defendant, that was

14 turned over to the defense in its entirety.

15   THE COURT: Okay.

16 BY MR. GRINDROD:

17 Q. So in your declaration you referred to the exploit as

18 a -- like a defect in the lock of an activating computer.

19 A. I did.

20 Q. And you note that what the exploit does is it essentially

21 would allow someone with the proper tool to pick that lock,

22 correct?

23 A. I don't know if I said "pick lock" -- I may have -- but

24 bypass the lock, yes, that's accurate.

25 Q. Okay. And, so, in this case for each of our clients the

D. Alfin - Cross

1 exploit was sent to our clients' activating computer.

2 A. It was downloaded to their computer, yes.

3 Q. It was sent from the FBI to their computer physically,

4 correct?

5 A. They downloaded it from the government's computer, yes.

6 Q. And, indeed, the exploit was sent every time that the NIT

7 was deployed, correct?

8 A. The NIT was only deployed once per user in the matter at

9 hand, so "every time" would be once.

10 Q. Agent Alfin, you just testified a moment ago that the NIT

11 was deployed a large number of times, although you didn't

12 want to specify the precise number.

13   THE COURT: There's probably many times when he's

14 talking about the hundreds of people that they participated

15 in.

16   MR. GRINDROD: That's correct.

17 BY MR. GRINDROD:

18 Q. And, so, what I'm asking you about, Agent Alfin, is all

19 of these people, not just our clients in this case, but in

20 the whole Playpen operation.

21   THE COURT: How is that relevant?

22   MR. GRINDROD: Well, Your Honor, the government is

23 now claiming that the exploit is so sensitive that it can't

24 be turned over. Even with a strong protective order, it

25 can't be reviewed by an identified expert in a safe

1 environment, even at FBI Headquarters, right? And now I

2 believe Agent Alfin will testify that this same code that is

3 so sensitive it can't be disclosed under strict controls was

4 sent out, I don't know, a hundred thousand times or so and

5 could have been recorded in transit.

6   THE COURT: I don't know about a hundred thousand

7 times, but --

8   MR. GRINDROD: Well, without them limiting the

9 number down, Your Honor, I think the Court has to assume --

10   THE COURT: A number of times, and what you're

11 saying is that since the people who received it can discover

12 the code --

13   MR. GRINDROD: Not discover it, Your Honor, it was

14 sent to them.

15   THE COURT: It was sent there, but can they

16 determine what the code was that they used to pick the lock?

17   MR. GRINDROD: Yes, Your Honor.

18   THE COURT: I don't know. Ask him. Can they?

19 BY MR. GRINDROD:

20 Q. Someone recording --

21   THE COURT: If you use the exploit to go on my

22 computer to determine information, can I know what that code

23 is that you utilized by looking at my computer?

24   THE WITNESS: The specific answer to that question,

25 Your Honor, is contained in the document that the government

1 has asserted is law-enforcement-sensitive. However, speaking

2 generally, there are a number of pieces of software that can

3 be used so that even if you do send an exploit to someone's

4 computer, even if they know it's happening, even if they try

5 to record it, there are certain pieces of software that could

6 prevent people from doing it successfully.

7   I'm not authorized to answer whether or not such

8 software was used in this case or how it would have been

9 used; however, the statement that if it is sent to your

10 computer you can see it and analyze it, that on its own is

11 not always accurate.

12   THE COURT: Well, I'm going to recognize now the law

13 enforcement privilege until I find out if there's any

14 materiality to it, and I'll look at that based on the rest of

15 the evidence that I hear in this case.

16   MR. GRINDROD: I understand, Your Honor. Just for

17 the record, I would note an objection to that.

18   THE COURT: I note your objection.

19 BY MR. GRINDROD:

20 Q. Agent Alfin, to your knowledge, did any of the people to

21 whom the government sent the exploit that now may or may not

22 be classified -- did any of those people have security

23 clearances?

24   THE COURT: Does that make any difference?

25   MS. YUSI: Objection, Your Honor; relevance.

1   THE COURT: Do you think somebody important may have

2 been on the Internet and wasn't prosecuted? Is that what the

3 question is? I hope it's political.

4   MR. GRINDROD: The government is claiming that this

5 information is now retroactively classified. They sent it to

6 thousands of people before, and I want to know whether they

7 made any effort to determine whether those people were

8 authorized to handle classified information. I guess it

9 wasn't marked "Classified" at the time, but --

10   THE WITNESS: The source code that you are seeking

11 in discovery was not sent to anyone.

12 BY MR. GRINDROD:

13 Q. Was the exploit sent?

14 A. Obviously, the exploit was.

15 Q. Okay. And there was no effort made on the FBI's part to

16 determine whether the people receiving the exploit had some

17 sort of security clearance or were going to handle the

18 exploit properly.

19 A. As the Court is aware, the users of the Playpen Web site

20 were not known to us before they were identified by the NIT,

21 so we did not know whether or not someone that we were

22 attempting to identify had a security clearance.

23   MR. GRINDROD: No further questions, Your Honor.

24   THE COURT: Thank you.

25   MS. YUSI: Just very briefly.

1   THE COURT: You don't have to be brief, but --

2   MS. YUSI: Just to follow up.

3   REDIRECT EXAMINATION

4 BY MS. YUSI:

5 Q. The exploit was sent, but that's not the source code,

6 correct?

7 A. Correct.

8 Q. The source code is what the defense is requesting,

9 correct?

10 A. Correct.

11 Q. Okay. Just to clarify something that Dr. Soghoian had

12 talked about and the Judge brought up about the IP addresses

13 being different on the PCAP report --

14 A. Dr. Soghoian testified that the data received by the

15 government was changed in transit.

16   THE COURT: That's what he said.

17   THE WITNESS: This is inaccurate and misleading.

18 The actual data --

19   THE COURT: He said the IPs were changed, as I

20 recall. Go ahead.

21   THE WITNESS: Again, that statement is misleading.

22 So the IP address that was used to identify the defendant did

23 not change. That, in my declaration, as it states, was not

24 changed in transit. So my declaration -- I believe it was

25 paragraph 19 -- is, again, true and accurate.

What Dr. Soghoian is referring to is the IP address of the government server that is visible in the data that we turned over. He suggests that because that IP address is not a public IP address that it had to change through multiple government servers. That statement is based on an assumption of how the government servers are configured. It is not supported by any testimony in the record or any evidence that the FBI or defense has put in.

A computer can have multiple IP addresses on it, both public and private, the distinction being a public IP address is used to communicate over the Internet. It is the one that was used to identify both of the defendants in the matter at hand. The actual network capture on the government's end occurred on a private IP address on a server connected to the Internet which also had a public IP address. The data that was turned over represents the government's private IP address.

Again, the important thing is that the actual data from the defendant's computers did not change in transit, nor did Dr. Soghoian allege that it did change in transit.

THE COURT: Am I to understand that the computer that sent the material to the government was a different computer than the Playpen computer?

THE WITNESS: So the government ran the Playpen Web site.

1   THE COURT: Correct.

2   THE WITNESS: The defendant connected to our Web

3 site --

4   THE COURT: Correct.

5   THE WITNESS: -- in the Eastern District of

6 Virginia. He downloaded the NIT and the exploit to his

7 computer.

8   THE COURT: Right.

9   THE WITNESS: And then the NIT sent that information

10 back to another government computer. It was not the same

11 computer that had the Web site on it.

12 BY MS. YUSI:

13 Q. And that's how it was designed, is that the NIT would

14 send the information to this third computer to -- as a

15 repository?

16   MR. GRINDROD: Objection, Your Honor; leading.

17   THE COURT: Objection sustained.

18   THE WITNESS: So that was how the operation was

19 designed. A user connects to the Playpen Web site, they

20 download the NIT from the Eastern District of Virginia, and

21 then the NIT sends the information back to another

22 government-controlled computer in the Eastern District of

23 Virginia.

24   THE COURT: So that computer would have been

25 different from the number -- the identification number would

1   have been different from the identification number for the

2   Playpen computer?

3   THE WITNESS: The actual Playpen Web site was not

4   relevant to the investigation. That was just where we hosted

5   the Web site, and we hosted it within the Tor network. So

6   the IP address of the Playpen server could not be publicly

7   seen, and it's not part of any of the information that's been

8   discussed today.

9   THE COURT: Well, what were the two IP

10 identifications that were utilized in the correspondence, or

11 the e-mails, or whatever it was that was transmitted?

12   THE WITNESS: One of them was the defendant's

13 computer --

14   THE COURT: Yes.

15   THE WITNESS: -- and the other one was the

16 government's computer.

17   And so the network data stream that we can see that

18 has been turned over to defense, you can see that entire

19 communication, which includes the information that the

20 government was authorized to collect.

21   THE COURT: All right. But when Mr. -- I don't

22 quite know how to pronounce his name, Soghoian -- when he

23 testified, he indicated that there was a difference between

24 the number of the IP number and what the government sent.

25 There were two different numbers. Or did he?

1   THE WITNESS: What Dr. Soghoian suggested was that

2 the data came back to the government computer --

3   THE COURT: Yes.

4   THE WITNESS: -- and then went to another government

5 computer.

6   THE COURT: Correct.

7   THE WITNESS: That is based on an assumption. That

8 is based on an assumption based on nothing that the

9 government has put in the record, and it is not supported by

10 any evidence that the defense has put on, either.

11   THE COURT: Well, how did the two IP numbers get

12 involved that he was speaking of?

13   THE WITNESS: So the NIT transmitted data back to

14 the government.

15   THE COURT: Yes.

16   THE WITNESS: And when it did that we could see the

17 defendant's IP address. The NIT knew where to send the

18 information, the government's IP address, because that

19 information is included in the NIT. And, so, the NIT knows

20 where to send the data to because it's included in that

21 package. And, so, it has with it the government's IP

22 address, so it knows where to initiate that connection to.

23 And, so, that is the data that is collected by the NIT, is

24 what can be seen in the evidence that has been turned over.

25 BY MS. YUSI:

1 Q.   And, just to clarify, Dr. Soghoian talked about headers,

2 correct?

3 A.   Yes.

4 Q.   And did any of the information change? What was he

5 referring to that changed?

6 A.   When Dr. Soghoian suggested that the PCAP data changed,

7 he was referring -- again, the PCAP data has a private

8 government IP address on it, not the public IP address, and

9 so that can be thought of as sending a package through UPS.

10 When it goes through a mail delivery facility, a sorting

11 facility, they slap another sticker on it, it goes where it

12 needs to go, but the package is never opened. It's not

13 ripped open and tampered with, in general.

14   And, again, as I described previously, we had a

15 number of precautions in place to prevent such tampering.

16 However, the important thing is that the data that was sent

17 from the defendant's computer was done so accurately, and we

18 captured it accurately.

19 Q.   And Dr. Soghoian agrees that nothing had changed in the

20 data.

21 A.   Dr. Soghoian agrees that there was no evidence that any

22 of the data was tampered with, is my recollection.

23   MS. YUSI: That 's all of my follow-up, Your Honor.

24   MR. GRINDROD: Your Honor, may I briefly address

25 those points with the witness?

1   THE COURT: Is it something new?

2   MR. GRINDROD: No, Your Honor. Well, it is limited

3 to points that were directly raised about what our expert's

4 testimony was and whether it should be credited, two quick

5 lines of questioning, Your Honor.

6   THE COURT: You've got two questions.

7   RECROSS-EXAMINATION

8 BY MR. GRINDROD:

9 Q. You just testified that when Dr. Soghoian said that,

10 based on his observations of the PCAP data, it looked like

11 the information that was sent back to the NIT went to a

12 public government IP address and then went to another

13 government computer, right? And you said that was

14 speculation; there was no evidence in the record of that,

15 right?

16 A. That's not an accurate quote, and the question doesn't

17 make sense from a technical standpoint. Can you restate it,

18 please?

19 Q. Sure. So you talked about Dr. Soghoian's testimony and

20 how he said that by looking at the PCAP data it was his

21 opinion that the information that was sent from our clients'

22 computer to -- was sent initially to an FBI server and then

23 to some other FBI server, and that he could tell that because

24 the PCAP data indicated that the IP address was associated

25 with this second private server, nonpublic government server,

1   remember?

2   A.   Yes, that is what he testified to.

3   Q.   And you said that was speculation and there was no

4   evidence in the record to support it, correct?

5   A.   I did.

6   Q.   But that is, in fact, what happened, right?

7   A.   No. As I stated, a server can have more than one IP

8   address on it. So just because the IP address changes

9   doesn't mean it went to another server.

10   Q.   Okay. So in this case the IP address changed. You agree

11   with that?

12   A.   Which IP address?

13   Q.   The IP address that's reflective of the government's

14   receipt of the information in the NIT.

15   THE COURT: Let's get a specific -- you know, I get

16   lost. I try to understand everything. So far I'm not sure

17   what IP address we're speaking of that changed.

18   There was an IP address, according to the expert,

19   the good doctor, that the numbers were different, okay? Not

20   the data was different, the numbers were different, the IP

21   numbers.

22   MR. GRINDROD: Right.

23   THE COURT: But I'm not sure it was material that

24   was transmitted to the FBI, so I don't know where it was

25   transmitted from or to whom it was transmitted. And we have

1 so many computers in this case I'm beginning to get confused

2 about the computers.

3   He indicated, the expert did, that there was a

4 computer that received the information; that is, it went into

5 the defendant's computer, got certain information,

6 transferred it to a government computer, which then

7 transferred it to another government computer, which

8 transferred it to the FBI. Is that what you understand his

9 testimony to be, or am I wrong?

10   MR. GRINDROD: I think there may be one extra

11 computer in there, Your Honor, but that is essentially --

12   THE COURT: Well, tell me what you understood it to

13 be so I can be on the safe side.

14   They obtained it from the defendant's computer.

15   MR. GRINDROD: That's correct.

16   THE COURT: And then it went to where?

17   MR. GRINDROD: It was routed through our clients'

18 wireless router, not directly but eventually went to an

19 FBI -- a government computer, and then, after that point,

20 went to either -- went -- there were some further transfers,

21 and between when it went to the FBI initially and when it was

22 subsequently transferred there was a change in the IP

23 address, of the receiving IP address, as displayed in the

24 PCAP data.

25   THE COURT: It wasn't the defendants' IP address.

1   MR. GRINDROD: Not that I was talking about there,

2   Your Honor. There's a separate issue as to whether the IP

3   address that --

4   THE COURT: The IP address that we're speaking of

5   was the government's IP address, correct?

6   MR. GRINDROD: In that instance, yes, Your Honor.

7   THE COURT: Okay. I just want to make sure.

8   Everything else there's been no contest over. We're in a

9   contest about what was received was a different IP address

10   for the government.

11   MR. GRINDROD: Well, and for our clients, Your

12   Honor, but that's for a slightly different reason. Well, a

13   very similar reason but based on --

14   THE COURT: I thought it was in the receipt of the

15   information that the FBI had --

16   MR. GRINDROD: It's both, Your Honor.

17   THE COURT: -- and it received it from a government

18   computer someplace.

19   MR. GRINDROD: Yes, that's correct, Your Honor.

20   THE COURT: And when they received it I understand

21   that we had an IP address that was different from some

22   government IP address, correct?

23   MR. GRINDROD: Yes, Your Honor.

24   THE COURT: Okay. It was not the difference of the

25   defendants' IP address.

1   MR. GRINDROD: It was that, also, Your Honor.

2   THE COURT: I never heard him testify about the

3   defendants' IP address. He's still here, so I'll ask him

4   about it.

5   Okay, that's it. Let's go. I'm pretty sure he said

6   it was the government's IP address.

7   MR. GRINDROD: Well, I think, Your Honor, that he

8   testified --

9   THE COURT: I don't want to "think" anymore.

10   MR. GRINDROD: Okay.

11   THE COURT: I'll find out what he said.

12   BY MR. GRINDROD:

13   Q. Let me ask you this question, Dr. Alfin:

14   So you made this distinction between the information

15   that was inside the package and the information that may be

16   displayed on the outside of the package, right?

17   A. There is a distinction. And, for the record, I just want

18   to be clear. I am not a doctor.

19   Q. So, Agent Alfin.

20   A. I just wanted to make sure I'm not --

21   THE COURT: We're not going back over all the

22   testimony. No more.

23   You've got one more question. You said you had two.

24   I've allowed you plenty. You have one more question, and

25   that's it. Make sure it's a good question.

1   BY MR. GRINDROD:

2   Q.   Even though you make this distinction between the

3   information that's in the package not changing, whereas,

4   perhaps the information on the outside did, in fact, the

5   information that allowed you to find my client was the

6   information on the outside of the package, correct?

7   A.   The information that allowed us to identify your client

8   never changed.

9   Q.   That's not what I asked you.

10 A.   It was on the outside of the package, but it never

11 changed.

12 Q.   Thank you.

13   MR. GRINDROD: No further questions, Your Honor.

14   THE COURT: Anything else from this witness?

15   MS. YUSI: Not from the government, Your Honor.

16   MR. GRINDROD: Not from the defense.

17   THE COURT: Thank you very much, sir. You may step

18 down.

19   THE WITNESS: Thank you, Your Honor.

20   THE COURT: Do you want to recall your witness, sir?

21   (There was a pause in the proceedings.)

22   MR. GRINDROD: I will briefly, Your Honor, just to

23 address that one point that we were talking about.

24   THE COURT: All right, I'm going to allow you to.

25   MR. GRINDROD: Your Honor, the defense recalls

1   Dr. Soghoian.

2   THE COURT: You're reminded you're still under oath.

3   CHRISTOPHER SOGHOIAN, Ph.D., recalled as a witness,

4   having been first duly sworn, testified as follows:

5   DIRECT EXAMINATION

6   BY MR. GRINDROD:

7   Q. Dr. Soghoian, were you present for the last exchange with

8   Agent Alfin?

9   A. I was.

10 Q. And there was some question as to which IP address we

11 were talking about, whether it was the government IP address

12 or our clients' IP addresses. Do you remember that?

13 A. I do.

14 Q. Can you explain to the Judge what, if any, IP address

15 changed?

16 A. Yes, Your Honor. There were two IP addresses that are

17 displayed in the PCAP file; the IP address of the computer

18 that ran the NIT, the defendants' computers, and then there's

19 an IP address for the government.

20   What I believe is that the IP address -- that both

21 IP addresses, in fact, changed between when the data left the

22 computer of the defendant and when the data was received

23 ultimately by the final government server.

24   THE COURT: All right. Now, it's very simple.

25 There has to be some documentation that you reviewed that saw

1   it. Where is that documentation?

2   THE WITNESS: So the government has provided us a

3   copy of the -- or provided counsel, who then provided me, a

4   copy of the PCAP file, which is the recording, and when I

5   looked at the PCAP file --

6   THE COURT: Well, let me have the PCAP file. I want

7   the PCAP file now.

8   THE WITNESS: The PCAP file is not in a form that is

9   easy for the -- for someone not skilled in the art to

10 understand. After this hearing, when I get back to their

11 office, I can provide a screenshot --

12   THE COURT: I don't want you to provide anything

13 when you get back to the office. I want to see the PCAP

14 thing now. I can employ an expert, don't worry.

15   Let me have the PCAP file right this minute.

16 Somebody's got it, the one that was shown to Mr. -- this

17 expert witness.

18   It's on a disk? There wasn't anything -- nothing

19 printed out?

20   MR. GRINDROD: This is exactly as we received it

21 from the government, Your Honor.

22   THE COURT: Is this what you reviewed?

23   THE WITNESS: Counsel e-mailed me a copy of the

24 files that were encrypted. I decrypted those files. I

25 believe the encryption was performed by the government.

1   THE COURT: Let me see what you e-mailed to the

2   witness.

3   MR. GRINDROD: It's the files that are contained on

4   this disk, Your Honor. I didn't --

5   THE COURT: Well, where is the copy of it?

6   MR. GRINDROD: Your Honor, I don't have a copy in

7   any other form than on this disk.

8   THE COURT: You don't keep copies of what you send

9   to people?

10   MR. GRINDROD: Well, Your Honor, it's --

11   THE COURT: You don't keep copies of what you send

12   in your mail?

13   MR. GRINDROD: It was -- it was -- I don't have any

14   other copy of this.

15   THE COURT: I didn't ask you about the copy of this.

16   What did you send to this witness? It wasn't that.

17   MR. GRINDROD: Your Honor, I dragged the files from

18   this disk into an e-mail, I sent that to Dr. Soghoian, I

19   sent, through separate means, an encryption code, and --

20   THE COURT: You sent an e-mail to him.

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

22   THE COURT: Okay. And you don't have a copy of the

23   e-mail?

24   MR. GRINDROD: Not with me, no, Your Honor.

25   THE COURT: I know you don't have it with you. The

1   computer isn't here.

2   MR. GRINDROD: That's correct.

3   THE COURT: So you have a copy. Tomorrow morning

4   get that copy to me.

5   MR. GRINDROD: Yes, Your Honor.

6   THE COURT: Now, that's a copy furnished to you by

7   the government?

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

9   THE COURT: And who encrypted it?

10   MR. GRINDROD: The government, Your Honor.

11   THE COURT: Oh, so the government gave you a copy.

12   Do you have a copy of what you gave him, Ms. Yusi?

13   MS. YUSI: Your Honor, I did not bring it. It's

14   actually a program file, I understand, and so it's not

15   something that you just -- it doesn't come up in a Word

16   document that you can print out. You actually have to look

17   at it along with other technology in order for it to appear

18   as anything.

19   THE COURT: Well, forget it. It's getting too

20   complex now.

21   So the only way you can determine it is to look at

22   it with other technology.

23   MS. YUSI: That's my understanding.

24   THE COURT: Okay. But you sent him an e-mail,

25   correct?

1   MR. GRINDROD: Yes, Your Honor, containing the file.

2   THE COURT: Are you sure somebody didn't hack your

3   e-mail on the way?

4   MR. GRINDROD: Well, we used encryption, Your Honor.

5   THE COURT: Oh, you used an encrypted e-mail?

6   MR. GRINDROD: Yes, Your Honor.

7   THE COURT: Oh, that's excellent.

8   Okay. We'll see where we're going. I'm still

9   worried about the materiality, but I am concerned about the

10 fact that IP addresses were changed. I'm curious about what

11 that is.

12   And I'm going to request you to see if you can't

13 copy the e-mail and send it to me. I'm asking the government

14 to send me a copy of the encryption of this concerning the IP

15 addresses.

16   MR. GRINDROD: And, Your Honor, if it also would be

17 helpful -- I know the Court wants the data itself, but

18 Dr. Soghoian showed me the data --

19   THE COURT: I don't want to hear from Dr. Soghoian

20 any more.

21   MR. GRINDROD: Not -- just --

22   THE COURT: That's it. He's testified. That's it.

23   MR. GRINDROD: Just the raw data.

24   THE COURT: I just want to see what's on the

25 encryption.

1   MR. GRINDROD: Will do, Your Honor.

2   THE COURT: I mean, whatever was encrypted. I want

3   to see the e-mail, the various -- the original document and

4   what the government says it gave to the defendant in relation

5   to some encryption, okay?

6   Anything else?

7   MR. GRINDROD: No, Your Honor.

8   THE COURT: Anything else, ma'am?

9   MS. YUSI: A follow-up, Your Honor.

10   CROSS EXAMINATION

11   BY MS. YUSI:

12   Q. The defendant's IP address that was sent in the package

13   to the FBI server --

14   A. That was received, you mean?

15   Q. That was received, yes, sent by his computer through the

16   NIT. The NIT sent it, correct?

17   A. The PCAP shows it was received, and if you're going to

18   ask me about the IP address, that changed along the way.

19   Q. Okay. But that's the IP address that Cox or the local

20   ISP -- went to the defendant's residence. Is that right?

21   A. Are you asking me if that's what is in the PCAP file or

22   if that's what left the defendants' computer?

23   Q. What's in the PCAP file contains an IP address that led

24   to the defendants, correct?

25   A. I believe so.

1   Q.   Thank you.

2   MR. GRINDROD: I have nothing further, Your Honor.

3   THE COURT: I don't have anything further. Thank

4   you very much. You may step down, sir.

5   All right. Tomorrow I want those furnished to me,

6   by 12:00 noon tomorrow, that e-mail you sent, the encryption

7   that you gave them, whatever that encryption was, and a copy

8   of this thing that was given to the government. I'm more

9   interested in the change in the IP address than anything

10   else.

11   In relation to the materiality, is there any other

12   evidence concerning the materiality, to the defense, of the

13   code?

14   (There was a pause in the proceedings.)

15   MR. GRINDROD: Nothing further from the defense,

16   Your Honor.

17   THE COURT: Anything else, Ms. Yusi?

18   MS. YUSI: Not from the government.

19   THE COURT: Insofar as the motion to suppress is

20   concerned, that is denied at this time. I will forward an

21   opinion. It will probably take maybe a couple of weeks to

22   get the opinion out.

23   As well, I'm going to look at this question of the

24   materiality of the information of the code. I'm having lots

25   of problems finding any materiality, but I want to look

1 through all of these -- I have not read the testimony that

2 was filed given in Judge Morgan's court, except that I did

3 not necessarily agree with everything in his decision.

4 Although, I found it a brilliant decision and a great law

5 review article; however, I must say -- and I mean that

6 sincerely. It thoroughly investigated the law.

7   Insofar as the materiality is concerned, I want to

8 look at what's testified to there, and then I can probably

9 give you a decision. I'll try to give you a decision, but I

10 can't get a written out because it's somewhat complex, and I

11 figure it will take a couple of weeks to get the opinion out.

12 It's not the only case I have.

13   Anything else?

14   MS. YUSI: Not from the government. Thank you, Your

15 Honor.

16   THE COURT: Now, the question is do you want to take

17 some time to argue this matter tomorrow morning?

18   MS. YUSI: Your Honor, I don't have anything to add

19 that the Court hasn't heard at this point.

20   THE COURT: Do you want to argue the matter

21 tomorrow, Mr. Grindrod or Mr. Cejas or Mr. Colgan?

22   MR. GRINDROD: Your Honor, unless -- I mean, we'd be

23 happy to address any concerns the Court has, but --

24   THE COURT: I'm not trying to -- I'm just giving you

25 the opportunity if you want to.

1   MR. GRINDROD: I appreciate it, Your Honor.

2   THE COURT: Okay. Thank you very much.

3   (The hearing adjourned at 6:02 p.m.)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Heidi L. Jeffreys, Official Court Reporter

```
 1                        CERTIFICATION

 2

 3         I certify that the foregoing is a correct transcript

 4    from the record of proceedings in the above-entitled matter.

 5

 6                             /s

 7                      Heidi L. Jeffreys

 8

 9                      July 14, 2016

10                           Date

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25
```