UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
IN TACOMA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	No. CR15-5351RBJ
	)	
vs.	)	
	)	
JAY MICHAUD,	)	
	)	
Defendant.	)	

MOTIONS HEARING

BEFORE THE HONORABLE ROBERT J. BRYAN
UNITED STATES DISTRICT COURT JUDGE

January 22, 2016

APPEARANCES:

Keith Becker
U.S. Department of Justice Criminal Division
Matthew Hampton
Assistant United States Attorney
Representing the Plaintiff

Colin Fieman
Linda Sullivan
Federal Public Defender's Office
Representing the Defendant

01:26:42PM time we would move for the admission of those for the
01:26:44PM record.
01:26:46PM MR. FIEMAN: Your Honor, I have no objection. But
01:26:47PM we should also move in 14, which is the same as Defense
01:26:52PM Exhibit A15 and A16. I would move for the admission of
01:26:56PM all of those --
01:26:56PM THE COURT: What numbers now? A15 and A16?
01:27:03PM MR. FIEMAN: Yes, your Honor.
01:27:04PM THE COURT: Do you have any objection to those?
01:27:05PM MR. BECKER: No, your Honor.
01:27:07PM THE COURT: All of those exhibits may be admitted.
01:27:13PM (Exhibit Nos. A15 & A16 were admitted.)
01:27:13PM MR. BECKER: One other issue, your Honor.
01:27:21PM Exhibits 1 through 5 are all documents that are currently
01:27:24PM under seal. We haven't had an opportunity to conference
01:27:26PM with the defense in order to work out those issues, which
01:27:29PM we will.
01:27:29PM THE COURT: They should remain under seal until we
01:27:31PM resolve that issue.
01:27:33PM MR. BECKER: That would be our request. We will
01:27:34PM confer on that issue.
01:27:41PM MR. FIEMAN: Your Honor, if the government is
01:27:43PM complete, we would call Dr. Chris Soghoian.

CHRIS SOGHOIAN

01:28:11PM Having been sworn under oath, testified as follows:

01:28:11PM DIRECT EXAMINATION

01:28:13PM By Mr. Fieman:

01:28:14PM **Q.** Dr. Soghoian, please spell your name for the record.

01:28:16PM **A.** Sure. My name is Christopher Soghoian. That is
01:28:20PM C-H-R-I-S-T-O-P-H-E-R, Soghoian, S-O-G-H-O-I-A-N.

01:28:28PM **Q.** And where do you work?

01:28:30PM **A.** I am the principal technologist for the Speech
01:28:34PM Privacy and Technology Project at the American Civil
01:28:38PM Liberties Union. Although I should clarify, I am actually
01:28:40PM volunteering here in my personal capacity.

01:28:43PM **Q.** Correct. We retained you as a technology expert in
01:28:47PM this case some time ago, correct?

01:28:48PM **A.** That's correct.

01:28:48PM **Q.** And are you being paid for your assistance?

01:28:51PM **A.** I am being reimbursed for my flights, and my hotel,
01:28:54PM and a per diem for food, but that's it.

01:28:56PM **Q.** What is your training and qualifications?

01:28:58PM **A.** I have a bachelor's degree in computer science from
01:29:02PM James Madison University. I have a master's degree in
01:29:06PM computer security from Johns Hopkins University. I have a
01:29:10PM Ph.D. in informatics, which is like a mix of computer
01:29:14PM science and law, from Indiana University. And I
01:29:17PM specialized there in studying the role that the telephone
01:29:22PM companies play in enabling government surveillance.

01:29:24PM **Q.** And have you testified in other court proceedings?

(/ Motion to Suppress) **Exhibit F-003**

01:29:27PM **A.** This is my first appearance in court, but I have
01:29:31PM acted as a defense expert for the public defender in
01:29:34PM Spokane, Washington. I have also -- I also have quite a
01:29:38PM bit of experience in training judges and explaining things
01:29:41PM to judges. I appeared at an event organized by the
01:29:45PM Federal Judicial Center in Washington, D.C. last year,
01:29:48PM explaining surveillance technology to judges. I also
01:29:51PM spoke to 60 Article III judges last year at an event
01:29:56PM organized by Georgetown Law School.

01:29:59PM **Q.** Slow down a little bit so the court reporter can get
01:30:02PM everything. You have also testified before the advisory
01:30:05PM committee on the Federal Rules of Criminal Procedure?

01:30:07PM **A.** I have, yes, sir.

01:30:09PM **Q.** And when did you do that?

01:30:10PM **A.** I think that was in the fall of 2014.

01:30:14PM **Q.** And have you ever had your publications or scholarly
01:30:17PM work cited by a court?

01:30:19PM **A.** Yes. My research and scholarship has been cited by
01:30:24PM several federal courts, including the dissent by the Chief
01:30:28PM Judge of the Ninth Circuit, Alex Kozinski. My research
01:30:32PM has also been cited by the state supreme court of
01:30:35PM New Jersey and the state supreme court of Massachusetts.

01:30:37PM **Q.** Now, as a consultant in this case, have you reviewed
01:30:41PM the discovery and materials that relate to Mr. Michaud's
01:30:46PM case?

Exhibit F-004

01:30:46PM **A. I have reviewed all documents you have sent to me,**
01:30:49PM **yes.**
01:30:49PM **Q. Did that, for example, include the NIT warrant**
01:30:52PM **application?**
01:30:53PM **A. I have reviewed the NIT warrant application, yes.**
01:30:56PM **Q. Let me just cut to the chase. Would you please**
01:30:58PM **explain to the judge what an NIT is and how it works?**
01:31:01PM **A. Sure.**
01:31:02PM **MR. BECKER: Objection, your Honor.**
01:31:03PM **THE COURT: Wait a minute. I didn't get the**
01:31:05PM **question.**
01:31:06PM **MR. FIEMAN: I asked him to explain to the court**
01:31:07PM **what an NIT is and how does it work.**
01:31:12PM **MR. BECKER: I would object to the foundation and**
01:31:15PM **speculation, your Honor. If this isn't based on any**
01:31:17PM **analysis of a network investigative technique in this**
01:31:20PM **case, i.e., the NIT in this case --**
01:31:23PM **THE COURT: A little more foundation is**
01:31:24PM **appropriate.**
01:31:25PM **By Mr. Fieman:**
01:31:25PM **Q. Dr. Soghoian, in the course of reviewing the**
01:31:29PM **discovery, have you, for example, reviewed all of the**
01:31:33PM **government's descriptions of the NIT that was deployed in**
01:31:38PM **this case?**
01:31:39PM **A. I have read the description of the NIT in this**

01:31:42PM warrant, and I have also read the description of the NIT
01:31:44PM in every public NIT application that is available -- that
01:31:49PM has become available over the last five or six years.
01:31:52PM Q. When you talk about NIT, that is a kind of term of
01:31:57PM art. It refers in the technology world to a specific type
01:32:01PM of code or technique; is that correct?
01:32:02PM A. The government describes this technology as a NIT.
01:32:06PM In the computer security community, which I am part of,
01:32:09PM this is generally described as malware or malicious
01:32:13PM software.
01:32:13PM Q. Can you explain what those are and why you describe
01:32:18PM it as malware?
01:32:20PM MR. BECKER: Objection, again, to the relevance of
01:32:23PM the characterization, your Honor. We are not talking
01:32:25PM about review of anything that actually happened in this
01:32:27PM case, the NIT in this case. We are talking now based on
01:32:31PM the witness' opinion and characterizations of how things
01:32:35PM can be labeled. I don't see how this has any weight or
01:32:39PM pertinence to the issues the court has to decide here. If
01:32:41PM the witness has examined something that was used in this
01:32:44PM case, as opposed to reading the documents, I might not
01:32:48PM object.
01:32:48PM THE COURT: I take this to be preliminary.
01:32:51PM Obviously, it needs to be tied up with the evidence in
01:32:55PM this case.

01:32:56PM By Mr. Fieman:

01:32:56PM Q. Let's use the word NIT. Does NIT have a meaning in
01:33:00PM the technology and cybersecurity world?

01:33:03PM A. I have been studying the government's use of what we
01:33:09PM now know to be NITs for several years. We did not know
01:33:12PM they called them NITs until we found one of the warrant
01:33:17PM applications a couple of years ago. But this general
01:33:19PM category of technology --

01:33:21PM Let me pause and say the FBI is not the only
01:33:24PM government agency in the world that seeks to use
01:33:28PM investigative techniques of this kind. There are many
01:33:31PM governments around the world that use techniques like
01:33:33PM this, and there are many companies that create
01:33:36PM special-purpose technology like this for these
01:33:40PM governments. These companies advertise these products,
01:33:42PM they advertise their features, they describe it in quite
01:33:45PM extensive detail.

01:33:46PM And so I have been researching this general category
01:33:49PM of technology for a number of years, and I can describe,
01:33:53PM again, in general terms, how it works. There are --
01:33:57PM Within the class of what the government calls NITs, there
01:34:00PM might be different kinds of NITs. Some NITs might do a
01:34:03PM very small subset of things, some might do more things.
01:34:06PM But I can tell you generally how these things work.

01:34:09PM The reason that people in the computer security

Exhibit F-007

01:34:12PM community describe this as malware is that -- Computers
01:34:15PM are built with cybersecurity protections within them.
01:34:18PM When you are browsing around on the internet, and you
01:34:21PM visit a website, under normal circumstances that website
01:34:24PM is only allowed to get your computer to do certain things.
01:34:29PM Malicious software, known as malware, tries to get your
01:34:32PM computer to do things that it would not ordinarily do.
01:34:36PM And in the case of this Tor software that we are
01:34:40PM discussing here in this case -- I have been
01:34:44PM researching -- I know the people who are behind the Tor
01:34:46PM Project. They are academics. They go to the same
01:34:49PM conferences -- the same academic conferences that I do.
01:34:53PM This is a ten-year-old project that has received millions
01:34:55PM of dollars of research funds to build a very secure piece
01:34:59PM of software that has one primary purpose, which is to hide
01:35:02PM the identity of people using it.
01:35:05PM Q. Let's slow down. Now you are talking about the Tor
network, in general, correct?

A. Yes.

01:35:09PM Q. Let's stop there. So you have been studying NITs for
01:35:13PM a considerable period of time, you have done research on
01:35:16PM it, and you have also reviewed all of the discovery in
01:35:18PM this case, correct?

01:35:19PM A. That's correct.

01:35:19PM Q. Now, you have also seen the various pleadings that

01:35:22PM the government has filed where they describe the NIT as
01:35:27PM seizing information from Mr. Michaud's computer?
01:35:29PM A. I have read that, yes, sir.
01:35:30PM Q. Can you just describe for the judge the process of
01:35:34PM how a NIT goes about doing that, in general layman's
01:35:38PM terms, without getting into any technical features, just
01:35:43PM in a bread-and-butter way how does that work?
01:35:45PM MR. BECKER: Objection, your Honor. I would renew
01:35:48PM my objection, your Honor. This is a lay witness'
01:35:51PM interpretation of the words and warrants in discovery. It
01:35:55PM is not based on any actual analysis of anything in this
01:35:58PM case. This is testimony that is of no value to this court
01:36:00PM in determining any of the issues here. We have made
01:36:03PM disclosure of certain technical information about the
01:36:06PM network investigative technique. If that's what the
01:36:10PM witness has reviewed, then fine. But right now we are
01:36:13PM just talking about looking at the legal documents. This
01:36:17PM witness' opinion about what legal terms mean -- or what
01:36:20PM terms in legal documents mean, again, I think this is
01:36:24PM irrelevant information that does nothing in order to
01:36:26PM illuminate any of the issues before the court.
01:36:28PM THE COURT: I think your objection goes to the
01:36:31PM weight to be attached. Go ahead.
01:36:35PM By Mr. Fieman:
01:36:35PM Q. Let's take up that objection for a moment. Have you

01:36:37PM consulted with another expert retained by the defense
01:36:40PM called Vlad Cirkovic?

01:36:44PM **A.** I have spoken to Vlad.

01:36:46PM **Q.** You are aware that we had actually requested from the
01:36:48PM government the entire NIT code, so you could do exactly
01:36:52PM the type of analysis that Mr. Becker says you have not
01:36:55PM done?

01:36:56PM **A.** It is true that if we had the complete code, that we
01:36:59PM would know a lot more than we know right now.

01:37:01PM **Q.** But based upon your consultations with Mr. Cirkovic
01:37:07PM as to the limited code that has been turned over by the
01:37:09PM government, and your extensive ten years of research into
01:37:12PM NITs and technology, have you formed an educated opinion
01:37:16PM about how both NITs in general and this NIT worked?

01:37:20PM **A.** I think I have a pretty good idea of how NITs work,
01:37:24PM in general. And then in both by reading the report that
01:37:26PM Vlad has prepared, and talking and exchanging emails with
01:37:29PM him, I think I have a good idea of what happened here.

01:37:33PM **Q.** Can you just describe that to the judge, to the best
01:37:35PM of your knowledge?

01:37:35PM **A.** As I was sort of explaining before, computers are
01:37:40PM programmed to have a certain basic level of cybersecurity.
01:37:45PM They only will allow websites to instruct them to do a
01:37:48PM limited subset of things. The NIT in this case targeted
01:37:52PM people who were using the Tor browser, and so it is

01:37:55PM necessary just for this moment to say that the Tor browser
01:37:59PM is programmed to protect even more information than your
01:38:02PM normal web browser would protect.
01:38:05PM Q. Let's just stop there. So if you have a Tor browser,
01:38:08PM and you are working on the Tor network, it is like you
01:38:10PM have added firewalls or security provisions in your
01:38:14PM computer to protect your privacy; is that correct?
01:38:16PM A. Yes. And not only do you have these additional
01:38:19PM protections, but in fact they slow down your experience.
01:38:22PM So people who are using Tor are experiencing a less rich,
01:38:26PM less fast internet, in exchange for these additional
01:38:30PM protections, which protect their privacy, both information
01:38:33PM about where they are going and information about -- and
01:38:37PM also protecting information about the websites themselves.
01:38:40PM Q. And those protections are on the user's computer; in
01:38:45PM this case it would be Mr. Michaud's computer, correct?
01:38:47PM A. Yes. There is a special web browser that runs within
01:38:51PM the Tor software, and it has been specially configured to
01:38:54PM protect itself from things that websites might try and do
01:38:58PM to force it to reveal identifying information, like an IP
01:39:02PM address.
01:39:02PM Q. When you say "force it to reveal," what is that
01:39:06PM process?
01:39:07PM A. So the Tor software has sort of two separate privacy
01:39:14PM protecting components. The first is the Tor network

01:39:18PM itself. There is a diagram in the book that the
01:39:22PM prosecution provided that sort of shows how things go
01:39:25PM through the Tor network. But, generally, instead of your
01:39:29PM computer contacting the website that you are visiting,
01:39:31PM with Tor your computer bounces the connection through a
01:39:34PM bunch of servers along the way.

01:39:36PM And the purpose of that is to hide the trail. So
01:39:38PM instead of passing a note directly to the judge, I would
01:39:41PM instead pass a note to the lawyer over there, and then the
01:39:45PM lawyer over there would pass the note to someone else in
01:39:46PM the back, and then eventually it would reach you. It gets
01:39:49PM there in the end, but it might take a bit more time to get
01:39:52PM there because of all these people passing it along. That
01:39:54PM is one of the privacy preserving features in Tor, which is
01:39:58PM that it hides the trail through the use of these servers.

01:40:02PM Secondly, the Tor browser -- It is a web browser --
01:40:06PM It is actually a variant of Firefox, which is a very
01:40:08PM popular piece of web browsing software that has been --

Q. Slow it down a little.

01:40:13PM A. Sorry. So there is a special customized version of
01:40:17PM the Firefox web browser that has been modified to be even
01:40:22PM more secure.

01:40:23PM Essentially there are tradeoffs on the internet.
01:40:26PM There are some features that make websites more
01:40:29PM interactive, that allow you to have rich media, video,

Exhibit F-012

01:40:32PM sound, an immersive experience. But those futures can
01:40:36PM also be exploited by malicious parties to learn private
01:40:41PM information about you.

01:40:42PM **Q.** When you say "malicious parties," you don't mean
01:40:45PM their intentions, but you are talking in code sense in
01:40:48PM terms of they are trying to get your computer to do things
01:40:50PM that you would not otherwise do?

01:40:52PM **A.** I'm sorry. "Malicious" is a term of art in the
01:40:58PM computer security community. When we say "malicious," we
01:41:01PM mean someone that is trying to do something without the
01:41:02PM knowledge or consent of the computer of the person that it
01:41:05PM is being done to.

01:41:07PM And so the Tor browser has been specially modified to
01:41:10PM turn off many features that regular web browsers have
01:41:15PM enabled. And by turning these features off, it reduces
01:41:19PM the number of ways that a website might try and learn
01:41:22PM private information about the person using the Tor
01:41:24PM software.

01:41:25PM **Q.** When you say it is private, it is information that
01:41:27PM the person, the user, at their computer, is not otherwise
01:41:30PM transmitting or wanting to make public; is that correct?

01:41:33PM **A.** Well, regular people don't transmit this information
01:41:37PM anyway. This is stuff that is being transmitted by your
01:41:41PM computer without your knowledge or consent to begin with.
01:41:44PM The Tor browser transmits less information to websites

01:41:47PM than a normal website -- than a normal web browser
01:41:51PM transmits.
01:41:52PM And then in addition to that, the Tor browser will
01:41:54PM refuse requests by websites to reveal information that a
01:41:58PM normal web browser would otherwise reveal.
01:42:01PM Q. So that is background. Now, based on your review of
01:42:04PM the discovery, your consultation, Agent Alfin's testimony
01:42:07PM today about the NIT and how it worked, can you just
01:42:10PM explain to the judge -- And really what we want to
01:42:13PM clarify is the locations at which various things happened.
01:42:18PM Can you do that step-by-step from where the NIT is first
01:42:22PM programmed through the capture of data?
01:42:25PM A. I will do the best that I can.
01:42:27PM Q. And go slowly.
01:42:28PM A. Remember, there is one big piece that we don't know
01:42:31PM the answer to, where we don't have some of the code that
01:42:34PM the government hasn't turned over. With the pieces that
01:42:36PM we do have, when someone browses to a website using the
01:42:42PM Tor browser, their computer requests a page. So if you
01:42:47PM are using the Tor browser, your computer asks a website,
01:42:50PM "Please give me this page." That website will then make
01:42:54PM it available and your browser will then go and take it and
01:42:58PM bring it back to your computer.
01:43:01PM In some cases that web page will contain text, and so
01:43:05PM the text will be displayed. In some cases there will be

01:43:08PM images, and the images will be displayed. In some cases
01:43:11PM there is computer programming contained within that
01:43:14PM website, and it will cause your computer to do some action
01:43:17PM before additional text might be displayed.

01:43:20PM Q. When Agent Alfin testified about the NIT running in
01:43:25PM the background, can you just clarify what that means in
01:43:29PM terms of what is being received on the computer in
01:43:32PM Washington?

01:43:33PM A. Sure. From what we understand, from what has become
01:43:40PM public, the web browser -- the Tor web browser in this
01:43:46PM case would have requested information about a particular
01:43:49PM page on this forum, one of these threads.

01:43:52PM Q. So the homepage of this website?

01:43:58PM A. The defendant would have logged in -- is alleged to
01:44:01PM have logged into the homepage, entered a user name and
01:44:05PM password. After that they would have clicked on a link to
01:44:08PM one of these forums. And every time there is a click that
01:44:12PM is happening -- every time someone is clicking on one of
01:44:15PM these links, their browser is requesting new
01:44:18PM information -- a new web page.

01:44:21PM According to what the special agent said, the NIT was
01:44:24PM only delivered after someone went into a thread and then
01:44:27PM clicked on a specific post. So at the point that the
01:44:31PM defendant is accused of clicking on that post, the website
01:44:36PM would have given his Tor browser a web page. Contained

01:44:40PM within that web page would have been an instruction for
01:44:43PM the Tor browser -- not for the defendant, but for the Tor
01:44:47PM browser.

01:44:47PM Q. Let's stop there. When you say "contained," can you
01:44:50PM see that on the web page?

01:44:52PM A. Can a human see it?

01:44:54PM Q. Would the user who is looking for, say, a picture on
01:44:58PM the internet, would they see those instructions?

01:45:01PM A. No, there wouldn't have been any instructions visible
01:45:03PM to a regular user. A high-tech sophisticated person might
01:45:08PM be able to figure that out, but a regular person just
01:45:11PM clicking around is not going to know there has been this
01:45:14PM new special code added to the web page.

01:45:17PM Q. So it is hidden code running in the background. When
01:45:20PM you say "sending instructions," it is not instructions to
01:45:22PM the user, in this case allegedly Mr. Michaud, it is
01:45:26PM instructions to the target computer?

01:45:28PM A. I want to pause on that word "running." The code
01:45:31PM does not run on the website. The code always runs on your
01:45:36PM web browser. So the website tells the web browser, "Do
01:45:39PM this." The code is downloaded to the web browser, the Tor
01:45:42PM browser in this case, in this case in the state of
01:45:45PM Washington. And it is only when the instructions are
01:45:47PM received by the Tor browser here in the state of
01:45:50PM Washington that they are run on that computer, and then do

01:45:54PM whatever the NIT is supposed to do.
01:45:56PM Q. And in this case, from the testimony you have heard,
01:45:58PM what exactly was the NIT supposed to do when it was
01:46:01PM inserted into the Washington computer?
01:46:04PM A. Okay. So this is where it gets a little bit
01:46:08PM complicated.
01:46:09PM Q. Go slowly.
01:46:10PM A. We don't know one of the important bits of
01:46:14PM information. The Tor browser is not supposed to give up
01:46:18PM its real IP address to anyone. That is the one reason
01:46:21PM that you use Tor.
01:46:22PM Q. And that Tor browser -- That is a program that is
01:46:25PM running on the Washington computer?
01:46:26PM A. On the computer of the defendant. The Tor browser
01:46:30PM would have been running there. The one thing the Tor is
01:46:32PM not supposed to do is give up your IP address. And if a
01:46:36PM website that you are visiting with a Tor browser asks for
01:46:38PM your IP address, the Tor browser will say no.
01:46:42PM If you think -- I know you have said think of the Tor
01:46:45PM browser like a firewall. Think of it more like a guard
01:46:48PM dog, a guard dog around a house. If the guard dog is
01:46:51PM trained to bark at every person who approaches the house,
01:46:55PM and someone approaches and the guard dog doesn't bark,
01:46:59PM well, you have to ask, what happened? Why didn't the
01:47:02PM guard dog bark? So something mysterious happened in this

01:47:07PM case that caused the Tor browser to even let the NIT do
01:47:10PM what it wanted to do, which was to collect this
01:47:13PM information that the Tor browser would never ordinarily
01:47:16PM give up.
01:47:16PM Q. So we don't know exactly the process because we don't
01:47:19PM have all the code. But just to clarify, the NIT is hidden
01:47:23PM code that is sent to the computer in Washington, correct?
01:47:26PM A. It is hidden code that is sent to the computer in
01:47:29PM Washington State that somehow causes the computer in
01:47:31PM Washington state to do something that it would not
01:47:35PM normally do.
01:47:35PM Q. So not only is the NIT going to Washington State, it
01:47:39PM is now giving instructions or overriding instructions on
01:47:43PM that Washington computer?
01:47:46PM A. Yes. If you want to use the guard dog analogy, you
01:47:49PM could think of it as maybe putting a sleeping pill in the
01:47:52PM dog food.
01:47:53PM Q. Now, once those override instructions are executed on
01:47:58PM the Washington computer after this delivery, I guess from
01:48:02PM Virginia, what is the next step in what the NIT, from all
01:48:05PM of your research and review of discovery, did?
01:48:08PM A. So once the NIT had bypassed the security controls
01:48:12PM within the Tor browser, it then had to collect information
01:48:16PM from the computer that it wished to send back. In this
01:48:19PM case it would be the IP address, which is an address that

01:48:22PM links the computer to a residential internet account. It
01:48:25PM would be what is called the MAC address, which is a unique
01:48:29PM serial number associated with your wi-fi card, programmed
01:48:33PM in the factory of the wi-fi card manufacturer. There
01:48:37PM would be some other information about the operating system
01:48:39PM that the special agent read out when he was on the stand,
01:48:43PM the user name on the computer, which version of Windows
01:48:46PM you are running, some basic information.

01:48:49PM But to learn that information, before the NIT could
01:48:51PM transmit that information back to the computer in
01:48:54PM Virginia, it would first have to go and collect it. So if
01:48:58PM you think of this as information that is in a house, well,
01:49:00PM maybe one piece of it is in the bedroom, and another piece
01:49:04PM is in the living room, one piece of it is in the drawer.
01:49:06PM The NIT first has to go and collect the information from
01:49:09PM different parts of the computer. And then once it has
01:49:13PM that information, then it would transmit it back to the
01:49:16PM server in Virginia.

01:49:18PM Q. So if I understand the process, the NIT bypasses
01:49:24PM security or overrides security features on the Washington
01:49:27PM computer. First step, right? And then second, it
01:49:30PM actually collects data or evidence on that computer. And
01:49:34PM then the third step, after it has seized the Washington
01:49:37PM data in this case, it then wraps it up in like a little
01:49:42PM evidence bag and delivers it to the FBI in Virginia?

01:49:45PM **A. That sounds right. Although I'm not sure about the**
01:49:49PM **evidence bag. It transmits it back to the computer in**
01:49:52PM **Virginia.**
01:49:52PM **Q. And then once that data has been transmitted back, it**
01:49:57PM **is stored, apparently, on an FBI server; is that correct?**
01:50:01PM **A. The special agent said that the server is under the**
01:50:06PM **government's control. I am not sure how much I can say in**
01:50:10PM **this room about where we think the server is or which**
01:50:13PM **company we think might have been running the server.**
01:50:15PM **Q. I don't want you to --**
01:50:17PM **A. A computer in Virginia.**
01:50:20PM **Q. Is it then fair to say after this search and seizure**
01:50:24PM **in Washington, then really what is going on is it is in**
01:50:26PM **like an evidence room in Virginia where they keep that**
01:50:28PM **evidence until they need it?**
01:50:31PM **MR. BECKER: Object to leading at this point, your**
01:50:33PM **Honor. I think we are just reiterating testimony.**
01:50:34PM **THE COURT: That is a fair objection.**
01:50:36PM **By Mr. Fieman:**
01:50:36PM **Q. Describe then what the storage in Virginia is about.**
01:50:38PM **A. Once the data has been transmitted by the NIT, I have**
01:50:43PM **no idea what the government would do with it. We know**
01:50:46PM **that it was transmitted to a computer in Virginia. At**
01:50:49PM **that point we have no -- They haven't turned over**
01:50:51PM **information about how it is stored, or who has access to**

01:50:54PM it, or whether it is printed on paper or stored live in a
01:50:58PM computer. We don't know how it is maintained.
01:51:01PM Q. Now, you had just briefly mentioned that there are
01:51:08PM parts of the code that are missing data, and so you have
01:51:12PM to be a little reserved about your opinions, correct?
01:51:14PM A. I do not know how the NIT was able to get the Tor
01:51:21PM browser to do this thing that the Tor browser would never
01:51:25PM normally do. The general way that one does this -- the
01:51:29PM general way of describing this is to exploit security
01:51:35PM flaws in software.
01:51:36PM In fact, when I started testifying here I used the
01:51:39PM term "malware." And in the computer security community
01:51:44PM the term "malware" really describes software that is doing
01:51:48PM things that the person whose computer it is running on
01:51:54PM doesn't know it is doing or doesn't want it to do. In
01:51:58PM many, many cases malware, to effectively function, first
01:52:01PM must exploit some security flaw in the software that is
01:52:05PM running on your computer, whether that is your web
01:52:07PM browser, a piece of email software, or PowerPoint, or
01:52:11PM Microsoft Word.
01:52:12PM All of these programs that we run on our computer, the
01:52:15PM engineers who write them do the best job they can, but
01:52:19PM sometimes they make mistakes. There are a lot of people
01:52:21PM out there that are looking to find these flaws. If you
01:52:24PM can find one of these flaws, you can write special code

01:52:27PM that takes advantage of the flaw, and then lets you run
01:52:30PM code on a computer that the computer probably shouldn't
01:52:33PM run normally, or obtain information that you wouldn't
01:52:36PM normally be able to get.

01:52:37PM Q. And you say not normally be able to get. Let me ask
01:52:41PM you this: Based on all your review of the discovery and
01:52:44PM the testimony, if the NIT had not been delivered to the
01:52:47PM Washington computer, and collected the data for the
01:52:51PM Washington computer, would the website otherwise have the
01:52:56PM IP address and other identifying data in the normal course
01:52:59PM of events?

01:53:00PM A. No. The Tor browser is programmed to protect those
01:53:03PM pieces of information.

01:53:11PM MR. FIEMAN: Your Honor, I just have one other
01:53:13PM brief area and then I will be able to wrap up.

01:53:14PM By Mr. Fieman:

01:53:14PM Q. From a technical standpoint, I want to ask you about
01:53:17PM when the NIT was sent to Washington, how it was deployed.
01:53:20PM You have reviewed the warrant application in this case --
01:53:24PM the NIT warrant application?

01:53:26PM A. Yes, sir.

01:53:26PM Q. You are aware the warrant application, I think,
01:53:29PM allowed for the FBI to deploy -- to send the NIT
01:53:35PM anywhere at the time people logged into the homepage; is
01:53:37PM that correct?

01:53:37PM **A. I am aware of what the warrant authorized, as far as**
01:53:41PM **one can be aware as a non-lawyer.**
01:53:43PM **Q. As of that point, the NIT could be deployed and**
01:53:48PM **collect all this information from anywhere in the world,**
01:53:50PM **correct?**
01:53:50PM **A. At the time that the NIT is delivered to the**
01:53:56PM **computer, the government doesn't know where the computers**
01:53:58PM **are. The computer could be in the state of Washington, it**
01:54:01PM **could be in Utah, it could also be in France or Spain.**
01:54:05PM **Again, the Tor network is a global network with hundreds**
01:54:09PM **of thousands of users located around the world. There is**
01:54:13PM **no way of knowing ahead of time where any one of those**
01:54:16PM **users of Tor might be.**
01:54:18PM **Q. Now, just from a technical standpoint, if the NIT**
01:54:21PM **could be deployed at the homepage, was there any technical**
01:54:26PM **reason that you are aware of why the website would have to**
01:54:31PM **retain, and publish, and distribute child pornography**
01:54:37PM **inside the website in order to accomplish the NIT**
01:54:40PM **deployment?**
01:54:40PM **MR. BECKER: Objection, your Honor. You have**
01:54:42PM **already ruled on this issue. This is not relevant to any**
01:54:45PM **of the suppression issues here.**
01:54:49PM **MR. FIEMAN: Your Honor, I just want to talk about**
01:54:50PM **the point of deployment, and that the point of deployment**
01:54:54PM **could have occurred from the homepage in all cases.**

01:54:56PM THE COURT: I'm not sure I understand the question
01:54:59PM here.
01:55:00PM By Mr. Fieman:
01:55:00PM Q. Is there any reason why all of the NITs, in order to
01:55:03PM collect IP addresses pursuant to this warrant, could not
01:55:06PM have been deployed simply from the homepage, that you are
01:55:10PM aware of?
01:55:11PM A. You can deliver a NIT from any web page on that site.
01:55:17PM The fact that the government chose to deliver it on a few
01:55:22PM select pages after people logged in or after people had
01:55:24PM clicked a few links, that seems, from a technical
01:55:26PM standpoint, arbitrary. They could have even put it on the
01:55:28PM homepage before people logged in or after people logged
01:55:42PM in.
01:55:46PM Q. Slow down. That's okay. You are an east coaster
01:55:51PM like me, Dr. Soghoian. Is there any point in sort of the
01:55:58PM physical process of the NIT search that you believe we
01:56:02PM have not covered that the court should be aware of?
01:56:06PM A. I am just thinking. For the issues that you guys
01:56:21PM have been litigating today, no.
01:56:26PM MR. FIEMAN: Your Honor, do you have any questions
01:56:27PM that we have not addressed at this point?
01:56:29PM THE COURT: No. Go ahead.
01:56:31PM MR. FIEMAN: Thank you, your Honor.
01:56:35PM CROSS-EXAMINATION

01:56:38PM By Mr. Becker:

01:56:45PM Q. Good afternoon, Dr. Soghoian.

01:56:47PM A. Hi.

01:56:48PM Q. Would you agree that the Tor Project does not
01:56:56PM guarantee perfect anonymity to its users?

01:56:59PM A. My understanding is that the homepage of the Tor
01:57:02PM Project tells people that it cannot deliver perfect
01:57:05PM security.

01:57:05PM Q. Right from the homepage of the Tor Project it advises
01:57:08PM its users that it cannot deliver, as you said, perfect
01:57:11PM security; is that correct?

01:57:12PM A. What I will say, though, is that the Tor Project is
01:57:16PM about ten years old. It has received millions of dollars
01:57:20PM of grants. It is the best thing that the computer
01:57:22PM security research community has come up with thus far.

01:57:25PM Q. It has some great uses, is that fair to say?

01:57:28PM A. The Tor Project is being used by Facebook, it is
01:57:33PM being used by newspapers, ProPublica, and many newspapers
01:57:38PM that now run whistle blowing websites. As I'm sure you
01:57:41PM know, the Tor Project was originally -- the technology was
01:57:44PM created by the U.S. Navy, the Naval Research Lab, and the
01:57:47PM U.S. government has been and continues to be the biggest
01:57:51PM funder of Tor.

01:57:51PM Q. As we said, it can be used for many laudable,
01:57:55PM positive purposes, correct?

01:57:56PM A. That is correct. And my understanding is it is also
01:58:00PM used by many law enforcement agencies so that they can
01:58:03PM conduct covert investigations online.
01:58:05PM Q. Do you agree it can also be misused for illicit
01:58:09PM purposes?
01:58:09PM A. That is a complicated question.
01:58:11PM Q. Is it?
01:58:12PM A. Yes. Because the original creators of Tor -- When
01:58:16PM the Navy created Tor, the purpose was to allow naval
01:58:20PM investigators to research people online so that they could
01:58:23PM investigate whatever crimes the Navy is researching
01:58:26PM without tipping off the world with the fact that the Navy
01:58:30PM is researching them. Now, if you have this technology
01:58:32PM that is protecting the privacy of naval investigators, and
01:58:35PM the only people who are using it are naval investigators,
01:58:38PM well, then you are not anonymous.
01:58:40PM Q. Are they the only people using Tor?
01:58:42PM A. No.
01:58:42PM Q. Would you agree that criminals use Tor?
01:58:45PM A. That is by design.
01:58:46PM Q. Criminals use Tor by design?
01:58:49PM A. When the Navy created Tor, and put the technology out
01:58:52PM there, they knew that they would have both good and bad
01:58:55PM users. If you only have one --
01:58:57PM Q. So you agree there are good --

01:58:59PM MR. FIEMAN: Your Honor, if Dr. Soghoian could
01:59:01PM finish his answer.

01:59:02PM THE COURT: You interrupted the witness.

01:59:05PM THE WITNESS: If you only have naval investigators
01:59:08PM using Tor, then the moment a website receives someone
01:59:11PM coming from Tor -- receives a request from someone using
01:59:15PM Tor, they know that it is the U.S. government. So the
01:59:19PM creators of Tor have a phrase they use, and they use it in
01:59:23PM research papers and elsewhere, it is that anonymity loves
01:59:27PM company. If you want to have a technology that lets
01:59:30PM people blend into the crowd, you need a crowd. And so the
01:59:33PM creators of Tor from day one knew that there would be uses
01:59:38PM of Tor that society would love and uses of Tor that
01:59:42PM society would not love as much.

01:59:44PM By Mr. Becker:

01:59:46PM Q. Let's back around to my question. We agree you can
01:59:50PM use Tor to mask your identity while committing crimes,
01:59:53PM correct?

01:59:54PM A. You can use Tor to mask your identity when you are
01:59:58PM online, and people can commit crimes online.

02:00:00PM Q. You can use Tor to mask your identity while you
02:00:03PM commit crimes online through Tor?

02:00:07PM A. Tor is a communication technology. That is like
02:00:11PM saying, can you use a car to commit a crime? Well, yeah,
02:00:14PM I guess so. But it is a regular technology that has good

02:00:17PM users and bad users. That doesn't mean the technology has
02:00:21PM some kind of morality associated with it. It is like
02:00:25PM FedEx, or the post office, or the telephone line, it is a
02:00:29PM core communications and transportation technology.

02:00:31PM Q. Sure. And I'm sure we would agree that no matter
02:00:34PM what sort of communication technology that criminals are
02:00:38PM using, law enforcement needs to take action based on
02:00:41PM whatever that technology is; is that fair to say?

02:00:43PM A. I think if law enforcement is concerned about people
02:00:47PM using Tor -- about criminals using Tor, I think the most
02:00:51PM rational approach would be to stop the U.S. government
02:00:54PM from funding Tor.

02:00:55PM Q. You don't want criminals who are using Tor to be
02:00:58PM investigated?

02:00:58PM A. No, I am not saying that. I am saying if you don't
02:01:01PM want criminals to hide their identity using Tor, then the
02:01:05PM U.S. government should stop writing the checks that are
02:01:09PM paying for Tor to be developed. If you are worried about
02:01:11PM the availability of a technology that lets people hide,
02:01:14PM and you don't think -- you think it is being misused, why
02:01:17PM are you paying for it? Just cut it off.

02:01:23PM Q. Let me ask you some questions about a different area.
02:01:26PM You haven't reviewed any computers or digital evidence
02:01:28PM related to this case; is that right?

02:01:29PM A. No, sir.

02:01:30PM Q. You haven't reviewed any of the computers that were
02:01:33PM seized from the defendant's home?
02:01:34PM A. No, sir.
02:01:34PM Q. You haven't reviewed any computer code that has been
02:01:38PM provided in discovery, correct?
02:01:39PM A. So Vlad, who is our other expert, he has reviewed
02:01:44PM computer code provided to him by DOJ. I have read the
02:01:48PM report that Vlad sent to me, but I have not personally
02:01:52PM reviewed the NIT code.
02:01:55PM MR. BECKER: Your Honor, I would make a Jencks
02:01:57PM request for that report, if we don't have it.
02:01:59PM MR. FIEMAN: I actually don't either, your Honor.
02:02:01PM I was unaware of any written report from Mr. Cirkovic. I
02:02:12PM am not sure there is one at this point. Although, there
02:02:14PM has been, obviously, a lot of conversations with the
02:02:15PM various experts on all sides. So I don't have a report to
02:02:21PM turn over. I will make inquiries, your Honor, absolutely.
02:02:22PM By Mr. Becker:
02:02:23PM Q. Dr. Soghoian, can you describe the written
02:02:25PM communications you have had with the defense expert about
02:02:26PM the analysis of the code?
02:02:28PM A. Sure. He sent me a few-paragraph email describing
02:02:31PM his initial analysis of the shell code.
02:02:34PM Q. Did you sign a protective order before you received
02:02:37PM that?

02:02:37PM **A. I agreed to a protective order when I first got**
02:02:42PM **retained. Whether I signed something, I don't remember.**
02:02:47PM **I am pretty sure I did. The public defender definitely**
02:02:51PM **sent me the protective order and asked me to agree to it.**
02:02:54PM **I would have to consult my records to see if I signed**
02:02:57PM **something and sent it back.**
02:02:58PM **MR. BECKER: Your Honor, I would request -- The**
02:03:01PM **witness has testified about a particular written**
02:03:03PM **communication during the course of this proceeding. I**
02:03:06PM **would request that and other communications.**
02:03:11PM **MR. FIEMAN: No objection, your Honor.**
02:03:13PM **THE WITNESS: Is there any way I can ask for a**
02:03:15PM **glass of water? Is that possible?**
02:03:46PM **By Mr. Becker:**
02:03:48PM **Q. Doctor, just a basic point. In terms of**
02:03:50PM **communications on Tor, it is correct that when a user**
02:03:54PM **communicates through Tor, the user is still using IP**
02:03:58PM **addresses in order to communicate, correct?**
02:04:02PM **A. Someone doesn't use an IP address to communicate.**
02:04:05PM **Q. IP addresses route communications, even through Tor?**
02:04:08PM **A. No, an IP address is a number assigned to you. You**
02:04:12PM **use the internet, and in particular the IP protocol, to**
02:04:16PM **communicate. But you don't use your address. It is not**
02:04:19PM **like -- When you write a letter to someone, you don't use**
02:04:21PM **your physical address to communicate, you use the post**

02:04:24PM office to communicate, and your address is printed in the
02:04:26PM top left-hand corner of the letter.

02:04:28PM Q. Very well. Does Tor not use IP addresses? Would
02:04:32PM that be a fair statement?

02:04:33PM A. Tor is what is called an overlay network. So there
02:04:37PM is a network on top of the internet.

02:04:43PM Q. Would it be correct to say using Tor means you are
02:04:46PM not using IP addresses to communicate?

02:04:48PM A. Again, as I said before, you don't use an IP address
02:04:51PM to communicate. You have an IP address. You use the IP
02:04:55PM protocol to communicate. I am sorry if it sounds like I
02:04:59PM am lost on these details, but you don't use an IP address
02:05:05PM to communicate.

02:05:06PM Q. You used and defined the term earlier that you called
02:05:12PM "malicious." You defined that as someone who -- an entity
02:05:17PM that was sending something or using something without
02:05:21PM knowledge or consent; is that fair?

02:05:24PM A. I'm sorry. Can you ask that question again, please?

02:05:26PM Q. Sure. You were defining a term earlier as
02:05:29PM "malicious." You said in your community you define that
02:05:33PM as something happening without knowledge or consent?

02:05:35PM A. That is a component of malware, yes, sir.

02:05:40PM Q. Would it be possible for that communication to be
02:05:44PM authorized and for you to still describe it as malicious?

02:05:49PM A. So the question is, can something be authorized and

02:05:51PM still malicious?

02:05:53PM Q. Yeah.

02:05:54PM A. Authorized by whom?

02:05:56PM Q. A court.

02:05:59PM A. I think in the computer security community malware is
02:06:05PM really about -- the definition of malware depends on the
02:06:08PM knowledge of the user and the consent of the user.

02:06:11PM Q. So you don't think the courts have the ability to --

02:06:21PM MR. BECKER: I will withdraw that. No further
02:06:22PM questions, your Honor.

02:06:24PM MR. FIEMAN: Very briefly, your Honor.

02:06:27PM REDIRECT EXAMINATION

02:06:30PM By Mr. Fieman:

02:06:31PM Q. Mr. Becker started with a very simple question. He
02:06:33PM asked you whether Tor -- Tor does not promise to deliver
02:06:36PM perfect security. Do you recall that?

02:06:38PM A. I do recall that exchange.

02:06:39PM Q. Is it also fair to say that a burglar alarm or a home
02:06:43PM alarm does not deliver perfect security?

02:06:45PM A. That is correct, and neither does the lock on my
02:06:48PM front door.

02:06:48PM Q. But the fact that it doesn't deliver perfect
02:06:51PM security, does that make it okay for somebody to break the
02:06:54PM lock on your front door and go in and take information
02:06:56PM from your home?

02:06:57PM **A. I am not sure if that is the right question for me.**
02:07:01PM **I will say --**
02:07:01PM **Q. Just as a matter of common sense.**
02:07:03PM **A. As an individual, no, it doesn't make it okay.**
02:07:08PM **MR. FIEMAN: Thank you. No further questions.**
02:07:15PM **THE COURT: It sort of sounds like no one should**
02:07:19PM **expect privacy with whatever is on their computer and on**
02:07:25PM **the internet?**
02:07:26PM **THE WITNESS: It is very hard for individuals to**
02:07:28PM **protect their privacy online. It is for that reason that**
02:07:35PM **the government has spent so much money trying to create**
02:07:39PM **technologies that let people protect their privacy. It is**
02:07:43PM **really hard for the average person to protect their**
02:07:45PM **privacy online. Those of us who are trying to protect our**
02:07:48PM **privacy, we have to work hard. Sometimes we get a slower**
02:07:52PM **internet experience. Sometimes we have to use software**
02:07:57PM **that is not as easy to use in order to protect our**
02:08:00PM **privacy.**
02:08:00PM **There is a huge amount of research that is going on in**
02:08:03PM **this space to create tools that let the average person**
02:08:06PM **protect themselves. I have spent much of the last few**
02:08:11PM **years trying to help the legal community to protect their**
02:08:13PM **privacy, trying to get law firms and the courts to employ**
02:08:17PM **basic privacy and security technology to protect what you**
02:08:21PM **all are doing. It is hard for the average person when**

02:08:24PM this stuff is so high-tech. My hope is over the next few
02:08:27PM years we will get better and easier technology that will
02:08:31PM protect people.

02:08:34PM THE COURT: We started this -- or in the middle of
02:08:39PM it, I guess, we came to the Tor instructions, or whatever,
02:08:45PM that say that it does not deliver perfect security. Is
02:08:49PM there any perfect security at this point, other than not
02:08:55PM putting it in there?

02:08:57PM THE WITNESS: In my community, and in the computer
02:09:00PM security community, we use concepts like defense in depth.

02:09:03PM THE COURT: What?

02:09:04PM THE WITNESS: Defense in depth. So rather than
02:09:08PM having one wall protecting your castle, you have ten
02:09:12PM walls. That way if the barbarians get over the first
02:09:15PM wall, they still have nine more they have to overcome.

02:09:18PM THE COURT: That is kind of what Tor does?

02:09:21PM THE WITNESS: The Tor has at least two walls.
02:09:23PM Probably over the next few years they are going to add
02:09:25PM some more. I was having lunch with a DHS official this
02:09:32PM week -- a Department of Homeland Security official, about
02:09:34PM the technology they are funding to help create even more
02:09:37PM walls. When you look at some of the data breaches that
02:09:41PM have happened in the last few years, the OPM breach, where
02:09:45PM all these federal employees had their private information
02:09:48PM lost and stolen by China, it is really hard to design

02:09:51PM secure software and to protect data.
02:09:54PM The old approach was let's keep the bad guys out. Now
02:09:58PM the approach is, how do we stop the bad guys before they
02:10:01PM get all the way to the inner room of the house, or how do
02:10:05PM we limit their access to information. There is an arms
02:10:11PM race going on right now between those who are trying to
02:10:13PM protect data and those who are trying to exploit data.
02:10:17PM This is a really interesting time. The unfortunate thing
02:10:20PM is for regular people it is really hard to protect
02:10:23PM yourself online.

02:10:25PM THE COURT: Okay. Thank you.

02:10:28PM THE WITNESS: Thank you, sir.

02:10:33PM THE COURT: Any other evidence to be offered here?

02:10:35PM MR. FIEMAN: No other evidence, your Honor, from
02:10:37PM the defense.

02:10:47PM THE COURT: Let me figure here a little bit. In a
02:11:17PM practical sense, you have about a half hour apiece to
02:11:20PM argue this, which should be enough. When you get to the
02:11:24PM U.S. Supreme Court they won't give you that much time.

02:11:29PM MR. FIEMAN: Who would you like to hear from
02:11:31PM first?

02:11:31PM THE COURT: Well, it is your motion, or motions.

02:11:39PM MR. FIEMAN: Your Honor, I think we are down to
02:11:41PM essentially the core issue around which everything else
02:11:45PM revolves. And it is really a brick and mortar issue. We