UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

HONORABLE DAVID O. CARTER, JUDGE PRESIDING

- - - - - - -

ECHOSTAR SATELLITE CORPORATION, et al.,	)	
Plaintiffs,	)	
vs.	)	No. SACV 03-0950-DOC
NDS GROUP PLC, et al.,	)	
	)	Day 4, Volume I
Defendants.	)	

_____)

REPORTER'S TRANSCRIPT OF PROCEEDINGS

Jury Trial

Santa Ana, California

Tuesday, April 15, 2008

Jane C.S. Rule, CSR 9316
Federal Official Court Reporter
United States District Court
411 West 4th Street, Room 1-053
Santa Ana, California 92701
(714) 558-7755

08-04-15 EchoStarD4V1

APPEARANCES OF COUNSEL:

FOR PLAINTIFFS ECHOSTAR SATELLITE CORPORATION, et al.:

T. WADE WELCH & ASSOCIATES
Attorneys at Law
BY: CHAD M. HAGAN
T. WADE WELCH
DAVID M. NOLL
CHRISTINE D. WILLETTS
Attorneys at Law
2401 Fountainview
Suite 700
Houston, Texas 77057
(713) 952-4334

FOR DEFENDANTS NDS GROUP PLC, et al.:

O'MELVENY & MYERS, LLP
Attorneys at Law
BY: DARIN W. SNYDER
NATHANIEL L. DILGER
DAVID R. EBERHART
Attorneys at Law
Embarcadero Center West
275 Battery Street
Suite 2600
San Francisco, California 94111-3305
(415) 984-8700
- AND -
HOGAN & HARTSON, LLP
Attorneys at Law
BY: RICHARD L. STONE
KENNETH D. KLEIN
Attorneys at Law
275 Battery Street
Suite 2600
San Francisco, California 94111-3305
(415) 984-8700

ALSO PRESENT:

JEAN-MARIE FEY, French Interpreter

I N D E X

EXAMINATION

SANTA ANA, CALIFORNIA, TUESDAY, APRIL 15, 2008

DAY 4 - VOLUME I

(7:58 a.m.)

(The following proceedings is taken outside the presence of the jury.)

THE COURT: We are on the record. All counsel are present, the jury is not present.

The Court is going to order all counsel not to refer to Judge Smith or make his presence known this morning. The reason for that is it would give, I think, the plaintiffs an unfair, prejudicial advantage. There is a concern on this Court's part that the present code has any true value. There have been patches, and, in fact, the swap has taken place. And by referring to Judge Smith as a special master and the, you know, black-box effect that he has, it gives added credence that this code might still be a super secret code that would have tremendous destruction for the company.

The Court doesn't believe at this present date, 2007, that the code has the same import it did back in 2002, 2003, and therefore, I think that a reference to a special master handling the code in this way gives a prejudicial effect to valuation if liability is reached, both for liability purposes and, of course, then the expansion into punitives if we get that far.

Second, I've imparted to the jury with counsel's consent this morning, at about 7:45, the wish to change out Tuesday to Monday and to be out of session on Tuesday so that that one juror, Mr. Bender, can keep his appointment with the county. They are considering that.

Lastly, Counsel, is there anything further before we resume?

(No audible response.)

THE COURT: All right. Thank you.

Kristee?

(The following proceedings is taken in the presence of the jury.)

THE COURT: All right. Good morning.

The jury is present. All counsel are present.

Counsel, thank you for your courtesy. If you'd please be seated.

The parties are present, and on behalf of EchoStar, Mr. Hagan, would you call your next witness, please.

MR. HAGAN: Certainly, your Honor. Plaintiffs call Christophe Nicolas.

THE COURT: Thank you.

Mr. Nicolas?

Thank you, sir.

And I assume that the gentleman with him is an

interpreter?

MR. HAGAN: That's correct, your Honor.

THE INTERPRETER: Yes.

THE COURT: Thank you.

And first, good morning.

THE WITNESS: Good morning.

THE COURT: And sir, would you be kind enough to raise your right hand, please.

CHRISTOPHE NICOLAS, PLAINTIFFS' WITNESS, SWORN

THE WITNESS: Yeah, I swear.

THE COURT: Thank you, sir. If you'd please be seated in the witness box to my left, and if the interpreter would like to come with him.

There should be a chair, or if you'd like to stand next to the gentleman.

Mr. Nicolas, would you state your full name for the jury, please.

THE WITNESS: Sure. So my name is Christophe Nicolas.

THE COURT: And Kristee, would you be kind enough to move that microphone a little bit closer to the gentleman.

And sir, would you spell your first name for the jury.

THE WITNESS: Yeah, C-h-r-i-s-t-o-p-h-e.

THE COURT: And would you spell your last name for the jury.

THE WITNESS: N-i-c-o-l-a-s.

THE COURT: And, sir, are you an interpreter?

THE INTERPRETER: Yes, I am.

THE COURT: Would you state your name for the jury, please.

THE INTERPRETER: My name is Jean-Marie Fey.

THE COURT: And would you spell your first and last name.

THE INTERPRETER: My first name is Jean-Marie, J-e-a-n-M-a-r-i-e, last name is Fey, F-e-y.

THE COURT: And what language are you interpreting?

THE INTERPRETER: I'm interpreting English into French and French into English.

THE COURT: All right.

Now, Mr. Nicolas, do you understand English well enough to testify in English, and then if you don't understand, use the interpreter, or would you prefer to have the entire examination conducted through the interpreter?

THE WITNESS: I'm ready to -- to try in English and use Jean-Marie in case we have a --

THE COURT: If you are willing to make that attempt, if you don't understand a question, there is no

inconvenience to the Court and the jury, just turn to the interpreter and ask for his help.

THE WITNESS: Okay.

THE COURT: But if we can have you attempt to testify in English, it removes, you know, a potential impediment, and hopefully those answers are clearly stated to you.

THE WITNESS: Sure.

THE COURT: So counsel will speak slowly to you.

Mr. Hagan, this is direct examination on behalf of EchoStar.

MR. HAGAN: Thank you, your Honor. Chad Hagan on behalf of EchoStar and NagraStar.

DIRECT EXAMINATION

BY MR. HAGAN:

Q Good morning, Mr. Nicolas. You've already introduced yourself to the jury, but can you tell us a little bit about yourself. Where do you live and work, sir?

A Yeah, so I'm a Swiss citizen, and I live, therefore, in Switzerland, a small town called Sacvey (phonetic) next to Lausanne where we have our headquarter based.

THE COURT: I am going to ask you to move that microphone even closer to you.

THE WITNESS: Okay. Sure.

THE COURT: And would you tap that microphone?

THE WITNESS: (Complying.)

THE COURT: Okay. Thank you.

Counsel.

BY MR. HAGAN:

Q And Mr. Nicolas, do you have a family there with you in Switzerland?

A Yeah, I'm married, my wife, Valerie. So we are married since 10 years, now. My wife Valerie is from Acrozi (phonetic), and we have two kids, Florian (phonetic), three and a half, and Loik (phonetic), one and a half.

Q And how long have you lived there in Switzerland, Mr. Nicolas?

A Since I was born, since '71.

Q Now, can you tell us a little bit about your educational background. What types of degrees do you hold?

A Sure. So I've done my -- my study also in Lausanne, and I have a bachelor and master degree in computer science. And I've done my study in the -- in the school called EPFL or Swiss Federal Institute of Technology in Lausanne.

Q Now, Mr. Nicolas, turning to your employment history, how are you currently employed?

A So I'm working for a company called NagraCard, and I am the senior vice president and CTO, or chief technology officer for that company.

Q And how long have you been employed with NagraCard?

A So I started in April '96, first with a company called NagraVision, also part of the Kudelski Group, and then moved to NagraCard when the company was created, I think, in '97, '98.

Q And prior to making your way up to senior vice president and chief technology officer for NagraCard, did you hold any other positions within the company?

A Yes, sure. I started as a software engineer developing software for -- for Smart Card, and then I move up as a project manager and then for R and D and vice president of R and D, and then I end up to -- to that position, the current position.

Q And when did you attain the title of senior vice president and chief technology officer within the company?

A So I -- let me think. Yeah, I -- I am a senior vice president since 2004 and CTO since last year.

Q Can you tell the ladies and gentlemen of the jury a little bit about your role within NagraCard. In other words, what are your daily job duties and responsibilities?

A Today?

Q Yes, sir.

A So today I'm managing a -- a small group of 50 people, which are mainly focused on innovation, so I'm managing innovation projects for the company, and the access is taking care of security, anything related to security with

our product on the technical side, so defining the -- the product design strategy for -- for our secure product.

Q And going back in time a little bit, you said that you initially started with the company as a software engineer; is that correct?

A Correct, yes.

Q Can you tell the ladies and gentlemen of the jury a little bit about what your role was within the company when you served as a software engineer?

A So I started to -- to work on the -- as I said, on the -- on the Smart Card development. First, doing some testing of the -- the software and developing some test equipment, and then I -- I stopped writing software, designing and writing software for -- for the Smart Card or the -- or the access card.

Q What type of business does NagraCard engage in?

A So NagraCard is mainly a company that is -- has main purpose to design, develop Smart Card software. And then we are also the -- the capability to produce the Smart Card. So we do the hardware production of the Smart Card or access card that we deliver them to our customer.

Q And can you explain to the ladies and gentlemen of the jury what you mean by Smart Card or access card?

A Sure. So a Smart Card stands for a plastic card, as any credit card, but has in there a specific microchip or

microprocessor, and that microprocessor has the capability to execute software as your computer. And within that microchip, we have various set of memory, and you will -- maybe about ROM memory, RAM memory or EEPROM memory. And those memory are use to store the software of the Smart Card or store the sensitive data or information needed to execute the -- the software.

MR. HAGAN: May I approach, your Honor?

THE COURT: You may.

BY MR. HAGAN:

Q Now, Mr. Nicolas, is that one of the Smart Cards that you are referring to?

A Yes, exactly. So you -- you see it's a piece of plastic, and you have -- that -- that piece is really the -- what we call the module, which is a golden plated module. And in there, you have that specific microchip, which is embedded or put in there, and that's really the part that will -- will be in contact with the receiver of the set-top box and to the communication with the receiver and the set-top box.

Q And can you explain to the ladies and gentlemen of the jury what you mean by receiver or set-top box?

A Yeah, to -- to have access to a digital TV or digital broadcasting, you will -- you will have to -- to install and hook your TV to a box, which I call set-top box or receiver.

And -- and the Smart Card will be inserted in the set-top box and -- and remain in the set-top box during the entire life of the -- of the box.

Q And the microprocessor, the small chip that you pointed out on the back of the Smart Card, is that where the memory is stored?

A Yeah, as I say, within that microchip, we have different memory, and we have the memory for the -- the software itself, but also for all the sensitive data, both what we call the access right condition, so which subscription you are entitled for and also all the -- the key, the secret key needed to decipher the message that you will receive in the box.

Q Are you familiar with the term "conditional access system"?

A Yes, I do.

Q Can you explain to the ladies and gentlemen of the jury what a conditional access system is and then what its role or function is.

A Sure. So the conditional access system is the part of the -- the software and system that we provide in -- in a big satellite system or DBS system. It's mainly the part that we'll manage, again, what I call the subscription. So for a given consumer, you will call and ask for some specific package, HBO package or basic package. And as soon

as you -- you ask for that, you will receive over the air a message that will put the corresponding right into the card.

And -- and the job of the conditional access system is, first, making sure that you have the right in the card, and if this is the case, it will entitle the -- the user to watch the corresponding TV channel. So that's mainly the -- the role of the conditional access system, manage your subscription and descramble the -- the message to give access to your TV programming.

Q Are you familiar with the process of pairing or marrying a particular Smart Card with a receiver?

A Yes, I do.

Q Can you explain to the ladies and gentlemen of the jury what that process involves?

A Yeah. So in our system, we deliver -- each Smart Card have what we call a unique ID or -- or a -- yeah, a card ID, so you see they're printed. You have a number, which will be unique per Smart Card. It's the same at the receiver level. On the back, you will have a label giving you a unique ID for the set-top box.

In our system, we have the capability to marry or pair both together, meaning that as soon as I insert my Smart Card, I know the number of the Smart Card and the number of the set-top box. I will ask the system to marry, to pair both together.

Q Who are some of the clients or customers that NagraCard develops these Smart Cards for?

A So in our conditional access system, we have for sure EchoStar as a customer, but we have various customer worldwide. I can mention in North America we have Bell Express View in Canada.

THE COURT: I'm sorry, you have who?

THE WITNESS: Bell Express View.

THE COURT: Use that mike.

THE WITNESS: Bell Express View, B-e-l-l, ExpressVu. And we have, then, various customer also in Europe such as Canal+, Virgin Media in the UK. We have some Polish customer, we have some Italian customer, such as Mediaset, and some Asian customer, also, Hong Kong Cable in Hong Kong, some in China. So it's really -- I think we have something like 130, 140 customer worldwide.

THE COURT: Now, let's stop just a moment.

Jane, do you need some of those spellings and maybe pronunciations to make sure you have that?

I might have you spell some of those companies. In fact, why don't you start with Bell Express. Is it B-e-l-l E-x-p-r-e-s-s?

THE WITNESS: Yeah, that -- that's the name I know. I don't know if it's the brand that they are using, but it's B-e-l-l, and Express View, E-x-p-r-e-s

V-e-i (sic) -- View, yeah.

THE COURT: And you mentioned Canal+. I know the court reporters have that spelling. In the UK, you mentioned a media company.

THE WITNESS: Yeah, it's -- it's called Virgin Media.

THE COURT: Can you spell that.

THE WITNESS: V-i-r-g-i-n Media.

THE COURT: And you mentioned an Italian customer.

THE WITNESS: Yeah, this one is called Mediaset, M-e-d-i-a-s-a-t (sic) -- media -- s-e-t, Mediaset -- e-t, yeah.

THE COURT: And finally, you mentioned a customer in Hong Kong, an Asian customer.

THE WITNESS: Yes. So the name of the customer is Hong Kong, as Hong Kong, and Cable.

THE COURT: Hong Kong Cable?

THE WITNESS: Yes.

THE COURT: Thank you very much.

Counsel.

MR. HAGAN: Thank you, your Honor.

BY MR. HAGAN:

Q Mr. Nicolas, who is NagraCard's largest customer in the United States?

A So the -- the largest customer that we have in -- in

United State is EchoStar on the DISH Network.

Q And as you understand it, EchoStar provides satellite programming to customers here in the United States?

A Yes, correct.

Q And that's under the trade name or the marketing name DISH Network?

A Yeah, that's my understanding, yeah.

Q Are you familiar with the company Nagra USA?

A Yes, I think Nagra USA is one of the Kudelski Group company, Kudelski in the U.S.

Q And are you familiar with the company NagraStar, one of the plaintiffs in this action?

A Yes, NagraStar is the joint venture between Nagra USA and EchoStar.

Q Mr. Nicolas, are you familiar with the company called NDS, the defendants in this case?

A Yes, I do.

Q And does NDS compete with NagraStar here in the United States?

A Yes, NDS is one of the main other conditional access system operator in the -- in the U.S.

Q Now, are you familiar with the Defendant NDS's largest client here in the United States?

A Yeah, my understanding is that DirecTV is the -- is the main customer of NDS in the U.S.

Q And based on your understanding, is it DirecTV is the major competitor here in the United States of Plaintiff EchoStar?

A On -- on the satellite side, that's my understanding, yes.

Q And you mentioned the company Canal+ earlier in your testimony. Can you identify that company for the ladies and gentlemen of the jury.

A Yes. Canal+ is a company part of the Vivendi Group, which is a big media company in Europe holding, I think, a few assets such as Universal Music. And Canal+ is also offering the same type of system, a satellite system in France, providing also TV programming to -- to customer as a customer in the U.S.

Q Are you familiar with the company called Sogecable, S-o-g-e-c-a-b-l-e?

A Yes, I do.

Q And what -- as you understand it, what type of business does Sogecable engage in?

A So Sogecable is also a media company, but this time in Spain, in Europe. And they're also one offering of satellite TV in Spain for Spanish customer.

Q Now, Mr. Nicolas, earlier you referenced a conditional access system, and that NagraCard through NagraStar provides part of EchoStar's conditional access system. I want to

focus our attention on the version of the conditional access system used by EchoStar during the 1996 to 2005 time frame.

A Okay.

Q As you understand it, is that system or was that system known as DNASP-II?

A Yes, we -- in -- in our jargon or slang, sorry for that, we -- we use a code name to -- to name the various family of conditional access system. And the -- the Kudelski company started with a first generation called DNASP, and then we developed the so-called DNASP-II family. That is the -- that was the one used by a customer at that time.

Q And are you familiar with what the acronym DNASP stands for?

A Yes, I do. So it stands for, if I recall correctly, "D" for digital, "N" stands for Nagra, advanced security processor. And Nagra is the brand name of Kudelski, so we have NagraVision, NagraCard. That's why we have Nagra in there.

Q Do you know when NagraCard first started providing the DNASP-II conditional access system to EchoStar?

A So we -- we started delivering DNASP-II Smart Card, and I think it was mentioning that in a family, we have various fashion of card. I think you -- you will hear about ROM 2, ROM 3, ROM 10, ROM 11. So all of those version are part of

the same DNASP-II family, okay? So we started delivering ROM 2 at the very beginning of EchoStar, so I think EchoStar started to broadcast in March '96. So that's probably the date we started delivering the card, maybe one or two months earlier to provide the card to and start the system.

Q Now, during the 1996 time frame, if I understood you correctly earlier, you were employed by Nagra as a software engineer; is that correct?

A That's correct, yes.

Q Did you participate in any way in the design of the DNASP-II system that's used by EchoStar?

A So when I -- I joined the company, the DNASP-II system as a system was already designed. As -- as I mentioned, I think I started in April '96, and EchoStar launch the system in March '96, so --

THE COURT: Excuse me, Counsel. Something is not clear, and it may be because DNAP can sound like DNASP. When you started in 1996, was the DNAP, D-N-A-P, system --

THE WITNESS: S-P.

THE COURT: -- in effect, or DNASP?

THE WITNESS: DNASP.

THE COURT: DNASP-II --

THE WITNESS: DNASP-II, correct.

THE COURT: -- was in effect in 1996.

THE WITNESS: What do you mean by "in effect"?

THE COURT: Was it --

(Discussion between interpreter and witness.)

THE WITNESS: Oh, in effect. So my understanding is that EchoStar started in March '96 using the DNASP-II system.

THE COURT: All right. Thank you.

Thank you, Counsel.

BY MR. HAGAN:

Q And that DNASP-II system, although it's referred to as one particular system, it had different generations or families of Smart Cards; is that correct?

A Yeah, that's correct. That's what I was trying to mention. In DNASP-II, we have various ROM version delivered to the customer.

Q Did you participate in any way in the development of any of those ROM versions or ROM family cards for the DNASP-II system?

A Yes, I do, so --

Q Can you explain to the jury what your role was in that development process?

A Sure. When I have join in April '96, the ROM 2 version was already out in the field, and the company was working on the so-called ROM 3. So I join and -- and started doing testing and -- and validation of that ROM 3 system. Then for the later one, ROM 10, ROM 11, I participate in the --

in the design and development of the card.

Q When you say you participated in the validation of the ROM 3 family of Smart Cards, can you explain to us what you mean by that.

A Yeah, mainly most of the source code of the software was already developed, and when I joined, I joined the team in doing what we call unitary testing of the code, so validating that the behavior of the code of the various feature working properly according to what we call the specification of the system.

Q And what do you mean by unitary testing?

A In -- in engineering, we call unitary testing, testing one feature at the time. So it's a unique test of that feature, and then we move to another feature, and so on.

Q Can you give us an example of one of those particular units that was tested during that process?

A Yeah, let me -- so we -- we, for example -- the card when inserted needs to -- to start communicating with the set-top box in a proper way and in -- and the communication follow a specific, what we call protocol way of talking to the -- to the set-top box, so there is various unitary testing to test that variable to make sure that the card follow properly the so-called protocol to talk with the set-top box.

Q Thank you, Mr. Nicolas.

Now, I want to turn your focus to the problem of satellite piracy. Are you familiar with that term?

A Yes, I am.

Q And can you give the jury a definition of satellite piracy in your words.

A Yeah. So I think we use the term "satellite piracy" as, I think, the main industry term to define any attempts to steal the -- the satellite TV programming.

Q And as -- as part of that process, is it your understanding that individuals have to circumvent or somehow find a way around the security features that are developed by conditional access providers?

A Yeah, that -- that's mainly the goal, to -- to have access, as I think we -- we mentioned that conditional access was there to make sure that the legit subscriber have access and the illegit (sic) one don't have. So to -- to steal programming, you need to find a way to circumvent or go around the conditional access system.

Q Is one way to look at the conditional access system somewhat of a lock that protects the programming that is being broadcast through that system?

A Yeah. We can say that, yeah.

Q And by the same token, is one way to look at satellite piracy attempts to break that lock or somehow pick that lock to steal the program?

A Yeah. Exactly, yeah.
Q How does satellite piracy affect NagraCard's business?
A So as a security provider, as soon as we have a security -- for sure, it will affect badly the reputation and the business of the -- the company.
Q When you started with NagraVision and then in NagraCard in the 1996 time frame, during 1996, to your knowledge, was that conditional access system which was used by EchoStar compromised?
A No, the -- the -- the system was not compromised at all in '96.
Q And is another way of -- of saying that, that the system was secure during that time frame?
A Definitely the system was secured and doing its job of securing the -- the satellite programming.
Q Now, how about the year 1997, was the system secure for EchoStar here in the United States?
A Yes, it was.
Q Now, moving to the year 1998, was EchoStar's conditional access system, that DNASP-II version, was that secure in the United States?
THE COURT: And that's DNAP?
THE WITNESS: DNASP.
MR. HAGAN: DNASP.
THE COURT: Once again, the initials.

MR. HAGAN: DNASP.

THE COURT: ASP, thank you.

MR. HAGAN: That's correct, your Honor.

THE WITNESS: Yes, I think for most of the year of '98, it was secure.

BY MR. HAGAN:

Q Now, based on your understanding, do you know whether or not the defendants in the year 1998 engaged in any efforts to reverse engineer or hack that security system?

A Yeah, that's definitely my understanding.

Q And what is that understanding based upon? Are there any documents that you're thinking of?

A Yeah, I think we have -- during that case, we've reviewed several document from NDS that clearly show that they were working on our system, on our Smart Card and defining how to first understand and then hack into our Smart Card.

Q Now, Mr. Nicolas, did there ever come a point in time where it came to your knowledge that DirecTV was approaching NagraCard or NagraStar in an effort to maybe try to replace the compromised technology of NDS?

A Yes, I do. We -- we were approach, I think it was, in '97 by DirecTV to -- to make a proposal to replace NDS conditional access system.

Q And based on your previous testimony, the year 1997,

that DNASP-II system used here in the United States was not compromised?

A Oh, yes, it was secure, fully secure.

Q Are you aware of any of the facts or circumstances surrounding DirecTV approaching NagraCard or NagraStar?

A What do you mean by --

(Discussion between interpreter and witness.)

THE WITNESS: Yeah, so my understanding was that DirecTV contacted NagraStar and Kudelski to replace NDS conditional access system due to the piracy ongoing on DirecTV.

BY MR. HAGAN:

Q Now, did you participate in any of those discussions with representatives for DirecTV?

A Yes, I was in several meetings both in the U.S. in Los Angeles in DirecTV premises and in Switzerland in our premises with DirecTV people.

Q Do you recall approximately when those meetings took place, the general time period?

A As I said, I think it started in end of '97 up to then at least December '98 or end of '98.

Q Now, did there come a point in time where the discussions went beyond just talking between the companies? In other words, did there come a point in time where DirecTV actually requested NagraStar or NagraCard to provide them

with a formal written proposal?
A Yes, we -- we clearly had been given access to all non-secret document that will allow us to analyze if we can design a system that will be compatible with the existing DirecTV system. And we were working tightly with their engineer to write what we call a white report, so it's really a full technical explanation on how we can provide a system -- replace their existing system without compromising the -- the normal behavior of the system without cutting the programming for the existing subscriber.
Q Did you participate in any way in developing that proposal or that plan?
A Oh, yes, I was involved in those discussion and also in -- in the work that we have done internally to prepare that report.
Q And can you give us just a summary of what your involvement was, not on the discussion side, but on the technical side?
A So as part of the Smart Card team, I was focusing on the -- on the Smart Card on security side making sure that we can understand existing box or receiver, and to make sure that we can design compatible Smart Card that will work into those existing receiver, DirecTV receiver.
Q Did DirecTV ever accept Nagra's proposal to swap out the NDS system with the Nagra system?

A So my understanding is that they were pretty happy with the report. We did, I think, one or two executive presentation to DirecTV management, top management there. And then we were almost ready to go, but finally were told that they -- they stopped the project, because they just sign a new extension of the existing NDS contract.

Q Do you recall which year that happened in?

A Yeah, it should be clearly after the report, so after the Summer of '98, so that year probably.

Q Turning back now to the DNASP-II system, did there come a point in time where you became aware that that conditional access system used by EchoStar in the United States became compromised?

A Yeah, I think the first rumor and then evidence that there was -- there has been a first successful attempt to attack our Smart Card was in October '98 when we have seen a publication of sensitive data coming out of our card, and that publication appeared, if I recall correctly, on dr7, which was one of the -- the internet website talking about DirecTV and -- at that time, DirecTV and then EchoStar pirating, piracy.

Q Do you recall the internet alias or screen name that was used to make that October 1998 publication?

A Yes, clearly, because that -- that nickname was not -- was something clearly to show us that they -- they were

aware of what was in the card, because the nickname was Nipper, and we had that name in our card. So it was a clear demonstration from the hacker that they have find a way to read information out of our card. It was a bit provocative, for sure.

Q Let me stop for a second. If I understand your testimony correctly, the DNASP-II system in the United States was not compromised in 1997, correct?

A That's correct, yes.

Q And during that time frame, you became aware that DirecTV began negotiations or discussions with NagraStar or NagraCard to replace NDS's technology?

A That's exactly the effect, yes.

Q And in then in 1998, DirecTV decided not to switch to Nagra; is that correct?

A That's correct, yes.

Q And at or about October of 1998, there was a publication on the internet under the alias "Nipper" that led you to believe the Nagra system had been compromised or someone had seen the secret codes, correct?

A Yes, that's correct.

Q Where in the code for the DNASP-II system did that secret phrase "Nipper" come from?

A Can you -- can you repeat the question.

Q Sure. You said that the word -- the secret phrase

"Nipper" was inside the card. Can you explain to the ladies and gentlemen of the jury where that was in the card?

A Yes, I -- I mentioned to you that we have that microprocessor or processor in the card and also various memory in the card, so the -- the "Nipper" word was stored in the memory that we call EEPROM or EEPROM, and -- and it was store in the chip.

Q Now, based on your understanding, what would an individual have to do in order to extract that secret code from the card?

A So to extract that, you need definitely to have access to that memory, so you need to -- to do what we call -- I'm sorry for the technical term -- an evasive attack. So you need to really dig into the chip to access that memory and that content.

Q Now, you said invasive attack; is that correct?

A Yeah. That's correct, yeah.

Q Did you ever become aware that the defendants performed any type of invasive attack on NagraStar's technology, the Smart Card?

A Yes, I do.

Q Do you recall approximately when that was?

A I think we -- when -- when we first see that publication on internet and also linked with some information that we gather at that time is coming from the

field, what we call the field to internet or -- or -- or a pirate, but also coming directly from a company such as DirecTV, that started to tell us that that was what NDS was doing on our system.

We were -- and I think by also the -- the various document that were seen in the -- in the discovery of that case, it's -- it was obvious, and it's obvious for us now, that they have the full equipment to do that kind of attack.

THE COURT: Counsel, I want to make certain that the jury knows what time frame we are still talking about. Is this still October of 1998, or is he discussing a later date?

MR. HAGAN: The -- the draft report is October of 1998, your Honor.

THE COURT: Let's confirm that.

BY MR. HAGAN:

Q Mr. Nicolas, as part of your work in -- in this case and preparing for your testimony, did you have an opportunity to review certain documents?

A Yes.

Q And was one of those defendants what -- what the defendants have called a Headend Report or Project Headend Report?

A Oh, yes, I've seen that great document, yeah.

Q And did you see a draft of that report that was dated

in or around October of 1998?
A That's correct, yes.
Q And did that Headend Report include the secret phrase "Nipper"?
A Yes, the secret phrase is -- is the -- is in the report with the exact location, also, of that secret -- secret phrase.
Q And if I understood your earlier testimony, that is the same month, October of '98, when the first Nipper publication was made?
A That's correct, yes.
Q Now, Mr. Nicolas, what is your understanding of the basis of the plaintiffs' claims against the defendants in this case?
MR. STONE: Objection, your Honor. That calls for speculation. Hearsay.
THE COURT: This isn't for the truth of the matter asserted. This is simply a summary of why he believes he's here testifying, what -- what this claim is. I'm not going to allow in the Complaint or the Cross-complaint or the Answer, et cetera, in this matter, it's hearsay. But you can give us a general understanding of what you believe the lawsuit is about.
The objection is overruled, Counsel.
BY MR. HAGAN:

Q Let me reask the question, Mr. Nicolas. What is your general understanding of the basis of EchoStar and NagraStar's claims against the defendants in this case?

A So my understanding is that we -- in the claim, we -- we say that NDS did a full attack and a reverse engineering of our Smart Card, and then used the -- the -- the secret information extracted during that process to feed or to provide information to hacker in the field, and therefore, help them to develop pirate Smart Card against EchoStar, our customer, EchoStar.

Q Now, Mr. Nicolas, based on your experience working with the DNASP-II system --

A Uh-huh.

Q -- was NagraStar and EchoStar, and with the help of NagraCard, able to combat the level of piracy of its system during the late '98, '99 to early 2000 time frame?

A So during that period, there was several attempt to use the -- the information that have been published to develop pirate devices, and versus those various pirate devices we started to do what we call -- and sorry for the technical term again -- countermeasure. So we -- we are developing solution and code that tried to circumvent the usage of pirate devices on EchoStar set-top-box system. And during that period, we did several attempt to -- to combat the various pirate devices, and sometimes we were successful,

sometimes not.

Q What types of efforts did NagraCard and NagraStar engage in, in order to try to combat that piracy? I think you referenced countermeasures. Can you explain for the ladies and gentlemen of the jury what those are.

A So what I'm calling a countermeasure is a specific designed code or message that we -- we develop, and then that we insert in the system, and that message will be broadcasted from the -- the broadcast center through the satellite and will reach all the set-top box and all the Smart Card. And at the reception of that message, the Smart Card will execute the code in there the exact same way as when you -- you access an internet website; sometimes you just execute a code to -- to have a feature.

So as soon as the message reached the card, we will execute the code, and that code can be a way, for example, to check that the Smart Card was not tampered with, or that code might be a way to have the set-top box checking that it's a legit Smart Card inserted on the set-top box and not a pirate devices.

Q Did you participate in any way for NagraCard in the development of any of these electronic countermeasures or ECMs?

A Yeah, I was on the team that was both in charge of developing and designing the Smart Card, but also developing

and designing the so-called technical countermeasure, and -- and then I was heading that team, also.

Q Now, did there ever come a point in time where NagraStar and NagraCard were unable to effectively combat the level of piracy for the DNASP-II system used by EchoStar in the United States?

A Yeah, I think we need to mention, I think, two key date there. The first time was when we saw the first attempt to modify the legit Smart Card, and -- and we've seen that appearing in 2000, but there was at that time only one commercial source of -- of the attack, so it means that there was only one source that have that capability. So at that time, you have to send -- take out your Smart Card and send that to a specific address, and you will receive it, I think, a few days or weeks later.

And the circum date, which is very important, is the publication at the end of this -- of 2000, so the -- the -- one or two publication that happened at that time. And that is key, because as soon as that was out, it was not only one single source that have that capability, but almost every -- every -- every person with some technical skill that can apply that technique against a card and create a pirate card.

Q Now, Mr. Nicolas, you referenced two events in that answer, and I want to break it apart and focus on each one

of them individually.

A Sure.

Q First, you said that in 2000, you became aware that there was one single source of reprogrammed EchoStar Smart Cards; is that correct?

A Yeah, I think it's late '99 or early 2000, yes.

Q Now, what do you mean by the term "reprogrammed EchoStar Smart Cards"?

A So when you want to have access to -- to the EchoStar programming, you -- you will try to find a way to have access to more than what you have paid for or even to -- not to pay to anything. And by reprogramming the card, there is a method that we -- we call or that the hackers start to call the "3M" to reprogram the card and extend the right that you have. So, typically, you just subscribe for one channel, which is a local channel. You send your card, and you receive your card back with the full entitlement, so all channel. And that's -- that's the type of hack or reprogramming that -- that was happening at that time.

Q And when you use the term "3M card," can you explain to us what you mean by that term?

A Yeah, I think that's -- that was a term developed by DirecTV at that time, and it stands for, I think, the Three-Musketeer, one for all, all for one. So the idea was, yes, you have right for one channel. You send it to receive

back for all channel. And when they started to apply that -- that type of attack on EchoStar, they just added the "E" in front of "3M," so it stands for E3M now, so just the same type of attack on EchoStar that used to exist on DirecTV.

Q Now, what is your understanding or -- what is your understanding of that one commercial source that was able to produce these 3M cards in the year 2000?

A So my understanding, there was only one technical source able to do that, and they started using one address or website to sell that, and slowly but surely expanded the sales networks using various internet website, but it was always the same technical source behind.

Q And what is -- was the name of that pirate website?

A So I think if I recall correctly, the way they organize their sales channel was that they used dr7 as the, quote-unquote, "independent website that will tell you where to go to get a good pirate card."

And then other website mention there will sell the Smart Card, and I think I recall one called Koinvision, I think, and -- yeah, there was two or three other that sell the same product at the end, but --

THE COURT: Could you spell Koinvision?

THE WITNESS: Yeah, if I recall correctly, it's K-o-i-n-v-i-s-i-o-n, Koinvision.

THE COURT: Okay.

BY MR. HAGAN:

Q Now, Mr. Nicolas, do you have any understanding of who the individual was who operated that dr7 website?

A Yeah, I think I was told that the guy managing that is -- is a person called Allen Menard.

Q Al Menard --

A Menard.

Q M-e-n-a-r-d?

A (No audible response.)

Q Now, the second thing that you reference or the second significant event was a posting at the end of December in 2000; is that correct?

A Yeah, that's correct.

Q Okay.

Steve, can we please give Mr. Nicolas a copy of what has been previously introduced in the trial as Exhibit 998.

And if we can pull that up on the screen for the jury.

Mr. Nicolas, if you could, take a moment to look at Exhibit 998, and let us know if you can identify it for the record.

A So is that the same that I'm seeing on the screen?

Q Yes, sir.

THE COURT: And remember, ladies and gentlemen, the jury box belongs to you. If you want to move down so

you have a closer view of the other monitor, you are more than welcome to.

Counsel, this exhibit has already been received, so if you want to blow up portions --

MR. HAGAN: Thank you, your Honor.

THE WITNESS: Okay. Yes, I recognize the -- the file.

BY MR. HAGAN:

Q And can you describe for the ladies and gentlemen of the jury what is depicted in Exhibit 998.

A So that's -- that file that I think I call "nipperclauz" is an explanation of what are the steps needed and what are the message needed to send to one of our card to take over control of the card and inject or inoculate a pirate software that we want to execute on -- on the card.

Q What's one example of this pirate software that you are referring to?

A Again, can you -- can you repeat.

Q Can you give us one example of this -- what you've called pirate software that you were referring to.

A Sure. So that -- that's the message that you need to send to the card, and in that message, you will embed the -- the pirate code that you -- you want to -- to -- to execute in the card. And one good example and first example, which is, I think, what we -- we see there, is a code that will

extract the -- the entire EEPROM, so it -- that code will read every byte, so every piece of information out of the EEPROM memory and send that back out of the card, so it's really a way to extract sensitive information in the card. But you can replace that pirate code by another one that can, for example, write into that EEPROM, so it's really a tool kit, to some extent, to do whatever you want with the card.

Q And what is the function of the EEPROM, E-E-P-R-O-M code in the DNASP-II card?

A Yeah, so the EEPROM memory is, let's say, I think the equivalent of your hard drive on your PC. It's the piece of memory that will keep your -- recall your data even if the card is removed from the set-top box. So the -- the other part of the memory ever not -- yeah, you cannot keep that -- that information in the memory, so we are -- we were using the EEPROM to store both the sensitive secret keys needed to decipher and descramble the programming, but also to store what I call the subscription and the corresponding right that you have paid for. So if we ever -- if you have paid for HBO, you will have that information in the EEPROM telling, yes, you have -- you grant -- you have been granted access to HBO, you can access the -- the TV programming.

Q And if you'll look down about the seventh or eighth line on Exhibit 998, there is an instruction that says "RX

4+4096 bytes," and you have "entire EEPROM"; is that what you are referring to?

A Yeah, exactly. That -- that will be the -- normally "RX" stands for "receiving," so that will be the result of the application of that message or what I call also that recipe on -- on the Smart Card.

So you will send -- you will -- you will resend the content inside the card and then send the specific message that you will see below, so it's really -- that part of -- of the byte, you will send that to the card, and what you will receive in return is 4,096 bytes, which correspond to the entire EEPROM memory content.

Q Now, if you'll look immediately above that line, there is a reference to ROM 3 Nagra Cam. Can you explain to the ladies and gentlemen of the jury what you understand that to mean?

A Yes, that refers to what I've mention, that the ROM 3 version of that DNASP-II family, and that was in '98, the card used to -- for all new -- new subscriber.

Q And when you use the term "recipe," can you describe for us what you mean by that term?

A For -- for me, I'm calling that the recipe, because it's not only the result of final attack on the card, but every step needed and -- and all the -- the ingredient, if you want, that you need to put to achieve that attack. So

you have -- you have mainly the steps. So you need to reset the card, wait for half a second, and then send that byte, and then you will receive that. And it explain you that you could replace the pirate code, give an ingredient to do another flavor of the attack, so that's why I call that the recipe.

Q And -- and we'll come back to the different flavors a little bit later on, but if I understand your testimony at this point, Exhibit 998, in your eyes, is what you consider a hacking recipe for the EchoStar Smart Card, correct?

A Yes, correct. That -- that was really the piece of information that give to the world the how to hack a Nagra Smart Card.

Q So it was basically instructions on how to hack that ROM 3 Smart Card?

A Yeah, definitely.

Q When did you first become aware of this Nipper posting, Exhibit 998?

A I think I received that posting from NagraStar during the Christmas break of December 2000, so if I recall correctly, that -- that file was posted in December 21st, something like that, and I should have received that through e-mail from NagraStar probably one or two days later, or maybe three days later.

Q And were you working during that time period, December,

late December of 2000?
A Definitely not in -- in Europe, the way we -- we organize, we usually close the company for one week. We are lucky, I know, for the Christmas break, so between usually December 22nd up to January 1st, 2nd, we are closed, but still working.
Q At -- at some time after you received this hacking recipe for EchoStar's Smart Card, did you engage in any efforts to try to analyze it to determine what it was?
A Yes. Yes, we do for sure.
Q And can you describe for the ladies and gentlemen of the jury what that analysis involved?
A So that analysis involved, really, understanding that file and understanding some of the other file that were published at the same times to -- to end up to the conclusion that it was first a working recipe on -- on our card, and it achieve what it needs to achieve, meaning to do whatever we want with our card.
Q In general terms -- and we'll come back a little bit later so that you can explain it in more detail, but -- but for this purpose, in general terms, can you describe how this hack recipe worked that's reflected in Exhibit 998.
A Yeah, in -- in very eye level, I think the -- the recipe that I use, several key information or behavior of the card that you need to first know and understand before

using or creating that recipe. So, you know, by sending that card, you will use a specific capability of our card to execute software in memory. That's the very first one that you need to understand and master before creating that recipe. Then, you need to understand the specific way we are managing the communication and specifically what we call the -- the buffer -- the communication buffer, and a specific way, which was called also the buffer overflow there.

You need to understand, also, a very, very undocumented and unknown feature of the hardware of the card, which we call the -- the partial decoding of the address of the RAM, or also, what we call the RAM Ghost Effect. And you need to understand, also, the way we manage the -- the internal copy of -- of those byte using what we call the index variable, or it's one variable that we use to -- to move data within the card.

Q And if I understand your testimony correctly, the way that this hack recipe works in Exhibit 998, utilizes four components, executing code and RAM, utilizing or overflowing the I/O communications buffer, utilizing what you coined the -- or you called the RAM Ghost effect, and then utilizing sophisticated knowledge of the index variable; is that correct?

A Yes, that's correct.

Q Now, Mr. Nicolas, did you ever become aware that the defendants engaged in efforts to create a hack recipe or methodology for EchoStar's conditional access system?

A Yes.

MR. HAGAN: Steve, can we -- can we give Mr. Nicolas a copy of what's been previously admitted -- forgive me -- previously admitted as Exhibit 98.

And can we get the defendants' Headend Report.

BY MR. HAGAN:

Q Mr. Nicolas, you've been handed a copy of what has been admitted in this trial as Exhibit 98, the defendants' Headend Report. If you could take a moment to just look at this and identify it for the record?

A Yes, that's -- that's what I've been shown and told that's the Headend Report, yes.

Q And have you had an opportunity to review the contents of Exhibit 98, the defendants' Headend Report?

A Yes, I do.

Q And based on your review and analysis of this document, what type of information does it contain; what does it describe?

A So I think it's -- the very first, let's say, 8 to 10 pages describe in great detail the way the software of our card was running and the way the hardware was also used. And on top of that, it's describing great detail, also, some

of the specific way our software was implemented and some of the weaknesses of the hardware in the card and the software in the card.

Q So this report describes, or at least the first 10 pages, components and functionality of the EchoStar and NagraStar conditional access system; is that correct?

A Yeah, correct, focusing on, let's say, trying to assess, really, the -- the security of the -- of the card and of the software implementation.

Q Now, when you reviewed this document, Exhibit 98, did you find any portion of it that described or talked about in any way the defendants' security system or conditional access system?

A Could you repeat that?

Q Sure. When you reviewed Exhibit 98, the Headend Report, did you find any portions of it that talked about the defendants' conditional access technology or improvements to their technology?

A No. I think that the report is fully focusing on our conditional access system, and more specifically, on EchoStar Smart Card that's used, for sure, our conditional access system.

Q And if I understood your earlier testimony, Exhibit 98 also describes the hack methodology that the defendants developed for EchoStar security system; is that correct?

A Yes, that's correct. The last 30 page out of 40 describe, really, the -- how to hack an EchoStar Smart Card.

Q And can you describe for us in general terms, again, the basic components or how the defendant hack methodology worked for EchoStar security system?

A Yeah, I can -- I can do that, but it might be useful maybe to -- I don't know if -- if I can use a flip chart or something to help the jury to -- to understand.

MR. HAGAN: May I approach, your Honor?

THE COURT: You may.

MR. HAGAN: Is this going to block your view, Judge?

THE COURT: Counsel, put it in the well.

MR. HAGAN: Okay.

THE WITNESS: May I go over there?

THE COURT: I am not sure that we can hear you.

I am not sure if this is necessary, Counsel. If he drops his voice, I -- I don't want to be in a position of having to stop the testimony.

THE WITNESS: The -- the point is that I can go without that, but it will be very technical, and I am not so sure it will be very useful.

THE COURT: Maybe we should use that, then.

(Laughter.)

MR. HAGAN: We can get him the microphone.

THE COURT: Will you speak in a loud voice --

THE WITNESS: I will try.

THE COURT: -- so we can hear?

THE WITNESS: I will try.

THE COURT: Thank you very much.

THE WITNESS: So let me maybe just draw, first, an example of how we can see the -- the RAM memory there, so it just will take me two second for that.

So you can represent a memory with a set of memory location that will be addressed by the -- the processor. And each time we address a memory location, we use an address. So let's say that that location is 0, 1, 2, 3, up to 9. And then let's say we -- we have the RAM. Let's stop there. So I think we mentioned four key things that needs to be known to create that recipe.

The -- one -- one of the first one is where we have put the communication buffer, and in our Smart Card, it was the very last part of the memory that was used to store that communication buffer.

So let's imagine that the buffer can store 3-byte data or 3 data, just to simplify. So each time we -- we send a message to the card, the card will store the message, and that's mainly what you have seen in the -- in the NipperClause in that buffer. So the very first information is that the way we are managing, the way the buffer -- if we

sell more than 3 bytes or more than the -- the size that the buffer can afford, we will write the data after that location. And in our Smart Card, we are told that that location doesn't exist. It means that if you address 10 or 11, there is no physical memory behind. So you are not harming the Smart Card, because there is no memory. There is nothing to address. So that was the -- the very first piece of information that you need to know, the way we manage the buffer.

Then I've mentioned, also, the RAM Ghost effect, and that's really the -- the key information that we were not aware before the attack and that we found out during our investigation. So as I told you, normally you should free address that position without harming anyone, because there is no memory there. But due to the RAM Ghost effect, the card, instead of writing at position 10 was indeed writing at position 0, there.

And as soon as you have overflowed the buffer, you are indeed writing not anymore at position 10, at location 10, but at location 0 in the RAM. And for sure, those are very sensitive location where you are just now impacting the normal behavior of the software. So that -- that's the second point, the RAM Ghost effect.

The third one is that we were using a specific index variable somewhere located in the memory. As

mentioned, it's in location 3. So that memory position needs to be modified to take over control of the card. So you need to keep going in term of buffer overflow.

So, first, you need to understand the buffer overflow, you need to understand the RAM Ghost effect, and you need to keep going writing bytes, position 10, 11, 12, 13, which is indeed 0, 1, 2 and 3, until you reach that specific index variable. And as soon as you reach that one, you will modify that value, and then allow you to take over of the stack. Sorry, that -- that's technical. So that's really a memory location there that will give you the -- the address where to jump in term of -- to execute the pirate software.

So as soon as you have modify that one, you are taking control of the stack, and then jumping into the -- the pirate code that you just inserted and execute that in RAM. So it was really the buffer overflow that you need to master, the fact that the card was narrowing or ghosting those location, 10, 11 and 12 where normally you having nothing into position 0, 1 and 3; 1, 2, 3, and that you cannot discover without doing a hardware attack of the card because we were not aware. It was not in the spec. It was not told by anyone.

Then, third one, you need to know exactly where that index variable is and reach that -- that byte.

And fourth, you need to have the capability to execute the pirate code that you have just injected there.

So -- and that's a very simplified view of what you need to understand, and without the -- the full reverse and the full attack and the full report, you cannot imagine or randomly find that attack.

I hope it was helpful.

BY MR. HAGAN:

Q Thank you, Mr. Nicolas.

So if I understood your demonstration, the Haifa hack, the one that the defendants developed, used the same four components, the I/O buffer overflow, the RAM Ghosting effect or address aliasing, the index variable and the ability to execute code in the RAM portion of the Smart Card that the Nipper posting, the hack recipe that we looked at as Exhibit 998; is that correct?

A Yeah, that's correct. Those four weaknesses are key characteristic of our card we mention, specifically in the Headend Report.

Q Mr. Nicolas, to your knowledge, as the senior vice president and chief technology officer of NagraCard, did the NDS defendants ever notify your company, NagraCard, that they were engaging in efforts to hack EchoStar's security system?

A Not at all.

Q To your knowledge, did NagraCard ever consent to the defendants engaging in efforts to hack NagraStar's conditional access system?
A Can you repeat that?
Q Sure. To your knowledge, did NagraCard ever provide any form of consent for the defendants' efforts to hack the technology used by EchoStar and NagraStar?
A No, definitely not that I'm aware of.
Q Would NagraStar -- I'm sorry, would NagraCard ever provide that type of consent to one of its competitors?
A I don't see the reason why to do that kind of things, but --
Q And the answer may be obvious, but can you explain to the ladies and gentlemen why that is.
A Yeah, I think NDS is using any information that can harm our business in -- in their marketing. So giving them access to our latest technology to do any kind of analysis will just, I think, give our competition key sensitivity information that they -- they will use against us in their marketing and sales pitch.
Q Now, in the wrong hands, would Exhibit 98, the defendants' Headend Report describing how to hack NagraStar --
A In the wrong hands?
(Discussion between interpreter and witness.)

THE WITNESS: In the wrong --

BY MR. HAGAN:

Q In the wrong hands, in other words, in the hands of satellite pirates --

A Uh-huh.

Q Could that information be used to damage or harm NagraCard and -- and the customers that use its security system?

A Oh, yes, definitely. That -- that's really a teaching book, so you have the first 10 pages that explain you in great detail what are the -- all the weaknesses of our card. And then you have the last 30 pages describing the fourth one that you need to use, and in exhibit, you have the exact same recipe that you need to -- to send to the card. And when I said "recipe," that it's -- it's how to use those four things, and then for sure we can use various flavor of the recipe, but it's exactly the same idea that is described there.

Q In the wrong hands, could that information, that hack recipe, if posted on the internet, be damaging or harmful to NagraCard and the -- and the clients that use NagraCard's security system?

A Yes, definitely.

Q And is that -- the hack methodology that you just described from Exhibit 98, in your opinion, is that in all

material respects identical to the hack methodology that was posted on the internet by Nipper in December of 2000?

MR. STONE: Objection. Lacks foundation, calls for an expert opinion.

THE COURT: Overruled.

You can answer that question.

THE WITNESS: Okay. Yes, definitely it's the exact same recipe using the exact same four key point.

BY MR. HAGAN:

Q To your knowledge, did NagraCard ever provide any type of consent to the defendants to distribute the information in Exhibit 98 to employees that were previously engaged in satellite piracy?

A For sure not.

MR. STONE: Objection. Assumes facts not in evidence.

(Interruption in the proceedings.)

MR. STONE: Objection. Assumes facts not in evidence.

THE COURT: I couldn't hear, Counsel.

Once again, question, please.

BY MR. HAGAN:

Q To his knowledge -- to your knowledge, Mr. Nicolas, did NagraCard ever provide the defendants with any consent to provide the information in Exhibit 98, the hack methodology?

THE COURT: The objection is overruled.

To your knowledge, sir.

THE WITNESS: No, for sure not.

BY MR. HAGAN:

Q If you look back at page 1 of the defendants' Headend Report, Section 2 is entitled "Hardware," and there is a reference to an SGS Thompson 16CF54 CPU. Can you describe for the ladies and gentlemen of the jury what that reference is?

A Yes, that's the -- we were using ST -- SGS Thompson at that time as a chief provider, and that's the -- the reference number of the hardware platform that we were using for ROM 2 and ROM 3.

Q Now, at the bottom right-hand corner of each page, there's a page number. It says "Page 1 of 40, 2 of 40." If you could, please turn to page 11 of the defendants' Headend Report.

There is a section entitled "Attack Tactics" or attack on the chip's hardware. Have you reviewed that portion of the defendants' Headend Report?

A Yes, I do.

Q And can you describe for the ladies and gentlemen of the jury what that section of the report describes?

A So those are really the -- the -- what I have call the key characteristic that you need to understand to then

develop the -- the recipe posted on the internet. So you -- you first explain the first attack on the chip that they have done to extract the very first time the code. Then you have the so-called RAM Ghost effect explained in great detail. Then you have the buffer overflow, or what they call there, the stack override, so really, the steps that they have tried to describe to reach the index variable and take control of the stack and --

THE COURT: Is that what you've previously referred to as the buffer overflow?

THE WITNESS: That's correct, yes.

THE COURT: Okay. Thank you.

THE WITNESS: And -- and then all the -- all those steps and exact location in the memory where to -- not to harm sensitive data that needs to remain in place to -- to still have the communication ongoing between the card and the set-top box or the reader.

BY MR. HAGAN:

Q Now, if you'll turn to page 14 of the defendants' Headend Report, at the bottom there is a notation that says "An example of such a message can be found in appendix F. Note that instead of the code used in this example to download the card's EEPROM contents, any code can be designed and written into"; do you see that part, sir?

A Yeah, I see that, yeah.

Q Based on your review of -- of the defendants' Headend Report and your analysis of the Nipper posting in December of 2000, do you have an understanding of what that language is referring to?

A Yeah, I think it's just mentioned the -- the appendix as one of the example that they were using to teach the attack method to the one reading the report. So you first have the technical explanation, then you have the -- the protocol, which is mainly the -- the table there, and then one or two example in appendix on how to use that protocol or recipe to attack the card.

Q Now, turning to the page 16 of the defendants' Headend Report, there are two sections that describe cloned cards. Can you identify for the jury what a cloned access card is or a cloned EchoStar Smart Card is?

A Yeah, I think that that -- those two paragraph describe how to create that so-called 3M card, which is mentioned. This is the classic 3M hack, so the very first one, the 352, explain how to -- to create all for one subscription, so a universal description or entitlement that will give you access to all the -- the channel.

And the second one, 353, describe you a way to -- to create a universal subscription for what is called pay-per-view events, so purchase on demand that you are doing on -- on the system.

So the very first one gives you full access to your -- your monthly description, and the second one give you full access to the pay-per-view event on the EchoStar system.

Q And Mr. Nicolas, further down on page 16 of Exhibit 98, there are two sections talking about a 3M hack in practice and DISH Network USA. Can you describe for the ladies and gentlemen of the jury what those paragraphs are discussing?

A I think it report the -- the step that they've taken to apply the recipe on an existing EchoStar set-top box and existing Smart Card, and they are describing what type of -- of set-top box and Smart Card were used to test that recipe, what was the result on the -- on the card EEPROM content, what was the initial subscription in the card prior applying the recipe.

There is various approach or method to -- to create 3M hack possibilities, and -- and -- and how to create those, a universal subscription and universal pay-per-view on the card.

Q If I understand your testimony correctly, this portion of the Headend Report is describing how to do a commercial hack of EchoStar's Smart Cards for the system, the DISH Network system here in the United States?

A Definitely, yes, it seems that they have apply the recipe, and they are just reporting that the recipe was working and what was the effect of the recipe on -- on the

Smart Card.

Q Now, turning to page 18 of the defendants' Headend report, appendix A, can you describe in general terms what this information is?

A So in the -- in the first column, you have what we call the address in the EEPROM where the -- the values that there are store or located.

And then the second column, the type, explain you what type of data you will find at each of those location and -- and also an ID to recognize the data. And then for each line, you have an explanation of what the data are used for in our Smart Card.

Q Now, Mr. Nicolas, if you could, turn to page 35 of the defendants' Headend Report, appendix F, and it is entitled "Stack override example, EEPROM contents download. Have you had an opportunity to review this section of the defendants' report?

A Yes, I did, yeah.

Q And can you describe for the -- the ladies and gentlemen of the jury just in general terms what this information is.

A So this information is the -- the same type of recipe that you need to send the same type of messages that you need to send to the card to apply the recipe and use those four key characteristic. It's -- it's just breaking into

one or two byte per line, because they -- they just added the -- the meaning of each byte and the explanation of which byte, why those byte are there and what they are entitled for. So the -- the NipperClause were giving the role data, that one, giving the same data, but with the clear explanation why those byte are there and what they are entitled for.

Q Now, Mr. Nicolas, I want to focus your attention back, now, on the Nipper post in December of 2000. Did that publication have harmful or negative effects on NagraCard and the conditional access system used in the United States by EchoStar?

THE COURT: Counsel, are you referring to both or one of those posts, which one?

BY MR. HAGAN:

Q Exhibit 998, Mr. Nicolas, the nipperclauz.txt file.

A So definitely had a big -- huge impact on us, because that recipe was given out to the world the first -- it was finger pointing on those four key characteristic and giving you directly the recipe to the world and how to apply that on -- on a Smart Card. And since then, instead of having one source of hack, technical hack, I think in a -- in a week or so, we have tens of people that have understood that recipe and how to apply that recipe on that card. And in two weeks, it was hundreds, and we -- we were starting to

see that recipe applied not only on EchoStar, but on other customers, such as the Soge Card one mentioned there.

So in a year, there was only one source that had the full exclusivity of that recipe. It took us almost two year to start to understand what was happening, and then yet you see that when that is published, in two days, you have tens of peoples that have that knowledge, so it was definitely awful for us.

BY MR. HAGAN:

Q Did NagraCard undertake any efforts to try to mitigate or to try to lessen the harm caused by Exhibit 998, the Nipper post?

A Yes. So at that time, we were starting also to understand what was happening in the card and what type of attack might be impacting the card. In -- earlier in 2000 we start understanding that RAM Ghost effect. Finally, we found out that -- that things, but still not understanding the full recipe and how to use that. And we have had access to other things, other information such as the -- the black box in October, November, so we are really starting to prepare ourself to do something. And the December 2000 caught us a bit by surprise, and we're to react quickly after that.

Q And in your answer, I think you identified two -- two additional events. One, that you began to understand the

RAM Ghost effect for the first time a little bit earlier in 2000. And then second, you acquired what you called the black box and analyzed it. Now, I want to break those --

A Sure.

Q -- apart and talk about each one.

What are you referring to when you say, "Earlier in 2000, we started to get some information about the RAM Ghost effect"?

A Yes, as I say, since 2000, there was one group that had the capability to ride into our card and create those E3M Smart Cards --

THE COURT: Just a little slower.

THE WITNESS: Sure.

THE COURT: A little slower.

THE WITNESS: Yeah.

So in 2000, there was one group that have that capability, and we were trying to understand how the hell they were able to write into our Smart Card. As with the full knowledge of the software, we were not able to find out how they -- they were using that. And we were pressuring our chipset provider, STMicro Electronic, to give us more information on the hardware itself to understand if we were missing something in our -- in our understanding of -- of the attack. And I think in a -- in a given meeting, I think it was something like, yeah, end of 2000, we were down in

South of France in -- in STMicro Electronic Premises starting to re-brainstorm with them and understand what -- what the piece of information was missing for us, and that's -- that's when we had access to one of their key design engineer, a nice -- a woman that -- that had designed the chip at that time, that between -- between their explanation tell us, "Oh, yes, we have that special RAM management. We have that special RAM decoding, partial decoding." And then we say, "What? Yeah."

And then we found out that there was one undocumented feature of the card that create that RAM Ghost effect. Instead of having the full decoding of the RAM, there was that partial decoding that created that when we were writing 10, we were writing in 0. And that was not communicated before, so it was a key piece of information that we as the developer of the card were only informed in -- in later 2000. So it started to open new track to investigate to -- to find out what was the -- the hack and what was the recipe that you can design having that new piece of information.

THE COURT: Now, just a moment, Counsel. Let Jane rest her hands for a moment.

When we get on the record, you referred to, "We were down in the South of," and then you named a location.

THE WITNESS: France.

THE COURT: "In an electronic premises starting to brainstorm with them." What was that location?

THE WITNESS: Yeah, we were in South of France in the location called the Rousset.

THE COURT: Spell that, please.

THE WITNESS: R-o-u-s-s-e-t, and it's an STMicro Electronic premises.

THE COURT: Thank you very much. Now we have that for our record.

And Counsel, please continue.

BY MR. HAGAN:

Q Do you recall approximately when it was that you attended this meeting in the South of France with STMicro representatives?

A I was not able to -- to find out the exact date, but I -- it was something -- let's say, if I have to guess, April, May time frame, May, June time frame of 2000, something like that.

Q And was this the first instance where NagraCard became aware of this property in the card called a RAM Ghost effect or address aliasing?

A Yes.

Q And who brought that information to your attention during that meeting?

A As I mentioned it was that -- that woman or girl which

was the head of the design -- the hardware design of the ST16 chip that was on the white board trying to explain us how the -- the hardware is behaving and give us that information.

Q Now, Mr. Nicolas, a moment ago, in addition to identifying this meeting, you also referenced a black box and reviewing a black box. Can you -- can you explain to us what you meant by that.

A Sure. So having that piece of information, we -- we started to define some hypothesis of how to use that weaknesses. So were just identifying one of -- out of the three other or four other key characteristic that you need to combine to -- to do that -- that recipe.

And in -- I think starting in September 2000 time frame, we started to also do more countermeasure, and we started to see movement on that E3M source of hack. The guys was starting to -- to be overwhelmed by the number of card he had to fix when we -- we were doing countermeasure, and he started to develop and sell box that will help him to -- to do more card at the time. So instead of going to any one location, he started to sell a black box, which is really a card reader that you can insert the card in, and that will apply the recipe in the card. So instead of having only one location, he was trying to set up multiple location to do that, and we were providing one of those box

through NagraStar that we had to analyze.

Q And did you participate in the analysis of that pirate device, the black box?

A Yes, that -- that was my team that did that. I just supervised the things. I didn't do it myself, but I -- I get the -- the result of that, yes.

Q Do you supervise the team of Nagra engineers in that project?

A Correct.

Q Now, can you -- just in general terms, can you describe for the ladies and gentlemen of the jury what that analysis was. In other words, how did you go about with a team of engineers analyzing this pirate device?

A So you receive a -- a black box or so-called Smart Card reader that is told to be able to apply that recipe to the hack. We were not aware that it was the recipe there at that time. And so what you do for testing, first, you -- you set or select a set of Smart Card that are in use in North America, definitely taking some of the EchoStar Smart Card, but also taking some other operator or customer that were in -- in North America. So we took a Bell ExpressVu Smart Card, we took a -- a GT Smart Card, so various one there. And then you insert each of those card in the -- in the black box and apply, quote-unquote, "the hack," and you just check the result. If the card get E3M'ed, so if the

card get the -- the full subscription right, you know that the black box is working. If there is nothing change in the card, you know that it's not working for that given operator.

Q Thank you, Mr. Nicolas.

Your Honor, I have about 30 to 40 minutes left in my examination. Would now be a good time to take a break?

THE COURT: This is a good time.

You're admonished not to discuss this matter amongst yourselves, nor form or express any opinion concerning the case. Why don't you take 20 minutes. We'll come and get you right around five minutes to the hour. Have a nice recess.

Sir, you may step down, and we'll see you at five minutes to 10:00.

THE WITNESS: Okay. Thank you.

And counsel, then, 20 minutes; 5 minutes to 10:00. Thank you.

MR. SNYDER: Your Honor, when we return, can we collect the exhibits that were given to the jury last week --

THE COURT: Yes, please.

MR. SNYDER: -- and then move two exhibits into evidence, 1000, and 1510?

THE COURT: Can we move those into evidence after

his testimony?

MR. SNYDER: That would be fine, your Honor.

THE COURT: All right. But we will collect those exhibits. Those were the 360 exhibits, weren't they?

MR. SNYDER: I believe that's right.

THE COURT: If you'd just make a notation and give it to Kristee, she'll give it to me, and we'll collect those.

MR. SNYDER: Thank you.

THE COURT: Thank you very much.

(Recess.)

(The following proceedings is taken in the presence of the jury.)

THE COURT: This would be the continuing direct examination by Mr. Hagan on behalf of EchoStar and NagraStar.

MR. HAGAN: Thank you, your Honor.

CHRISTOPHE NICOLAS, PLAINTIFFS' WITNESS, RESUMED

DIRECT EXAMINATION (Continued.)

BY MR. HAGAN:

Q Now, Mr. Nicolas, a little bit earlier this morning, you testified about some of the harmful effects that resulted from this December 2000 Nipper posting. We looked at it, and it's Exhibit 998. I want to go back to that for just a moment. You testified that as a result of that post,

NagraCard began to develop certain ECMs and software patches to try to correct that problem. Can you explain to the ladies and gentlemen of the jury what you are referring to with that -- the term "software patch"?

A I think -- as I told before, we have the capability to write a specific software that will insert in the system, and that code will be sent as a message through the satellite and reach the Smart Card there. So by doing that, we have the capability to load an extra piece of software in the card that would be installed in the EEPROM or to execute -- execute that piece of software in the ROM to do some check of the video of the card.

Q And did you participate in the development of that software patch?

A Again, it's -- I was leading at that time the team in charge of developing, designing the -- those type of patches, so I -- I did, to some extent, participate in the design and development of that software.

Q And do you recall approximately when it was that NagraCard finished that software patch to try to correct the problem exposed in the NiPpEr2000 -- or the December 2000 NipperClause post?

A So it probably took us one or two months to finish the -- the -- the first attempt to fix that -- that issue, so it took us probably until, let's say, mid-February 2001

to do that.

Q And once that software patch was developed, did Nagra launch that ECM, or I'm sorry, that software patch?

A So the way that we do that is NagraCard develop that, put that in the file that is delivered to NagraStar, and NagraStar is in charge of launching that software.

Q And can you explain to the ladies and gentlemen of the jury how that software patch or any software patch is deployed for EchoStar's system?

A So the file containing that software is delivered to NagraStar, then inserted in the Headend of EchoStar, so the broadcast center of EchoStar, and broadcasted through the -- to all of the Smart Card and set-top box.

Q Was that software patch in February of 2001, was it effective to try to combat the piracy that resulted from the December 2000 Nipper posting?

A Yeah, to somewhat -- yes.

Q And what do you mean "somewhat"?

A So first, you need to understand that we need to develop a software patch for each ROM or revision, so you will need -- you will need a dedicated software patch for ROM 3, but you will need also, to be successful, a dedicated one for ROM 2, and so on. So at that time we didn't find any means to fix the ROM 2 because we were not able to find enough room or memory space in ROM 2. I think there was

something like 20 bytes left on that card, and you cannot do a patch or fix with that memory. And we did one for ROM 3, and that patch was successful for some times to prevent the -- the usage of the recipe as it was published in December 2000. But since then, multiple flavor of the recipe started to appear, and multiple targets started to appear, and to do a successful patch, you need to understand which target you are -- you are targeting. And before it was easy, quote-unquote, easy; you have one target, one source.

Since January 2000, you have multiple source, and you don't know if that source is just one card for the own usage of the user or 1,000 card or 100 card, so selecting the right one is almost impossible, and fighting all of them is impossible.

Q So if I understand your testimony correctly, as a result of the December 2000 publication of that hack recipe, different pirates were able to develop different versions or what you call different flavors of that hack recipe; is that correct?

A That's correct, yes.

Q And the specific software patch developed and launched in February of 2001 was not effective to attack all of those different flavors of the hack recipe; is that correct?

A Yes, that's correct. It limited the usage of the

recipe, but as you clearly understand, I've explained the RAM Ghost effect, which is a hardware within the card, and by no means we can find a software that will fix a hardware weakness in the field. You cannot change the hardware no matter what. There is no magic there.

Q Was NagraStar or EchoStar eventually able to fix that hardware?

A No.

Q What did they have to do?

A So to fix a hardware, the only option that you have is to swap, to change -- exchange that hardware.

Q And when you refer it to "swap" or "change," what are you -- what is being swapped?

A So the Smart Card itself is being removed from the -- the existing Smart Card is being removed from the set-top box, and the subscriber will receive through the mail a new Smart Card that he will have to swap or insert back in the set-top box.

Q So as a result of the different flavors that derived from the December 2000 Nipper posting, EchoStar and NagraStar were forced to swap out the DNASP-II system; is that correct?

A That's correct.

Q Excuse me.

What was the name of the new system that NagraCard

developed to replace the DNASP-II system?
A So the DNASP-II system was replaced by a system called DNASP-III, which is not surprising, but then we used the code name "Aladin" for that system.
Q Aladin, A-l-a-d-i-n; is that correct?
A Yes.
Q Now, Mr. Nicolas, when you first saw or became aware of the December 2000 Nipper posting, the hack recipe, that we looked at as Exhibit 998, at that point in time, did you know who the individual was posting under the alias "Nipper" responsible for that hack?
A Could you repeat the question?
Q Sure.
A Which one are you --
Q Exhibit 998, the Nipper hack recipe, which you referred to as the hack recipe, when you saw that, when it was brought to your attention in December of 2000, did you know at that time who Nipper was?
A On the investigation side, it was NagraStar that was in charge of that, and my understanding is at that time, I think -- NagraStar already felt that it was clearly Christophe --
MR. STONE: Objection. It's hearsay. We have a witness from NagraStar coming.
THE COURT: Counsel, more foundation. Just how he

knew is hearsay.

MR. HAGAN: Okay.

BY MR. HAGAN:

Q And I understand from your testimony that that's NagraStar --

THE COURT: That's not the answer concerning Christopher Tarnovsky at this time. Let's find out what the foundation for that opinion is, Counsel.

(Live reporter switch with Debbie Gale.)

-oOo-

-oOo-

CERTIFICATE

I hereby certify that pursuant to Section 753, Title 28, United States Code, the foregoing is a true and correct transcript of the stenographically reported proceedings held in the above-entitled matter and that the transcript page format is in conformance with the regulations of the Judicial Conference of the United States.

Date: April 16, 2008

_____

JANE C.S. RULE, U.S. COURT REPORTER

CSR NO. 9316