

1

2

3

4

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA  
SOUTHERN DIVISION

5

6

7

8

HONORABLE DAVID O. CARTER, JUDGE PRESIDING

9

- - - - -

10

EHOSTAR SATELLITE CORP., )  
et al., )

11

Plaintiffs, )

12

vs. )

No. SACV-03-950-DOC  
DAY 13, Vol. IV

13

NDS GROUP PLC, et al., )

14

Defendants. )

15

16

17

18

REPORTER'S TRANSCRIPT OF PROCEEDINGS

19

Santa Ana, California

20

April 30, 2008

21

SHARON A. SEFFENS  
Federal Official Court Reporter  
United States District Court  
411 West 4th Street, Room 1-053  
Santa Ana, California 92701  
(714) 543-0870

25

APPEARANCES:

SHARON SEFFENS, U.S. COURT REPORTER

♀

1

FOR PLAINTIFF EHOSTAR SATELLITE CORPORATION, ET AL.:

2

3

T. WADE WELCH & ASSOCIATES  
BY: CHAD M. HAGAN  
CHRISTINE D. WILLETTS  
ROSS WOOTEN  
WADE WELCH  
Attorneys at Law  
2401 Fountainview

4

5

April 30, 2008 volume 4 kummer Hasak.txt  
Suite 700  
Houston, Texas 77057  
(713) 952-4334

6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

FOR DEFENDANT NDS GROUP PLC, ET AL.:

O'MELVENY & MYERS  
BY: DARIN W. SNYDER  
DAVID R. EBERHART  
Attorneys at Law  
275 Embarcadero Center West  
Suite 2600  
San Francisco, California 94111  
(415) 984-8700

-and-

HOGAN & HARTSON  
BY: RICHARD L. STONE  
KENNETH D. KLEIN  
Attorneys at Law  
1999 Avenue of the Stars  
Suite 1400  
Los Angeles, California 90067  
(310) 785-4600

ALSO PRESENT:

David Moskowitz  
Dov Rubin

SHARON SEFFENS, U.S. COURT REPORTER

3

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14

INDEX

PAGE

PLAINTIFF'S WITNESS:	DIRECT	CROSS	REDIRECT	RE CROSS
(None)				
PLAINTIFFS' EXHIBITS:		MARKED		RECEIVED
(None)				
DEFENSE WITNESSES:	DIRECT	CROSS	REDIRECT	RE CROSS
MR. KUMMER (Continued)		4	21	43
RUEVEN HASAK	47			
DEFENSE EXHIBITS:		MARKED		RECEIVED

(None)

15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

SHARON SEFFENS, U.S. COURT REPORTER

4

15:13:32 1 SANTA ANA, CALIFORNIA; WEDNESDAY, APRIL 30, 2008; 3:00 P.M.  
2 (Jury present.)  
3 THE COURT: The jury is present. Counsel are  
4 present. The parties are present.  
5 This is cross-examination by Mr. Welch on behalf  
6 of Echostar.  
7 MR. KUMMER, DEFENSE WITNESS, PREVIOUSLY SWORN  
8 CROSS-EXAMINATION  
9 BY MR. WELCH:  
10 Q Mr. Kummer, could you tell us a little bit about  
11 yourself before we get into your examination? Where are you  
12 from?  
13 A I grew up in Florida. I went to college at Florida  
14 Atlantic University. I graduated in 1979. I was married to  
15 my wife in 1980. I have been married almost 28 years. I  
16 have three children ages 18, 21, and 24.  
17 Q Where do you currently reside?  
18 A In Highlands Ranch, Colorado.  
19 Q How long have you worked for the Echostar group of  
20 companies?  
21 A I have been there for 15 years, since the beginning of  
22 1993.

23 Q I think you testified earlier that you had involvement  
24 in developing the DBS system, correct?

25 A Yes. I was hired as one of the first employees to

SHARON SEFFENS, U.S. COURT REPORTER

♀

5

15:31:18 1 focus solely on the digital system. Before that, Echostar  
2 built the big backyard dishes and analog satellite  
3 receivers. I was hired to start the digital system. I  
4 spent about a year looking at different compression  
5 technologies and conditional access vendors, chipset  
6 manufacturers and selecting those, and then I focused on  
7 building the actual set-top-boxes that we used at Echostar.

8 Q Now, Echostar launched its direct broadcast service in  
9 March 1996.

10 Are not those the set-top-boxes that you were  
11 instrumental in designing?

12 A Yes.

13 Q That's what we are here to talk about in litigation  
14 today?

15 A Yes.

16 Q When we left off -- when Mr. Snyder left off on his  
17 examination of you, he was talking about an issue called  
18 free-to-air. Do you recall that?

19 A Yes.

20 Q He kept asking about piracy at an intolerable level.  
21 Do you recall that?

22 A Yes.

23 Q Was the piracy at an intolerable level due to FTA, or  
24 was it an intolerable level due to something else?

25 A It was an intolerable level because all of the secrets

SHARON SEFFENS, U.S. COURT REPORTER

♀

6

15:32:35 1 of the system had been compromised when it was placed on the

2 Internet, and the free-to-air was a culmination of that. It  
3 went from originally being mainly modified Smart Cards to  
4 emulator devices to free-to-air. When you add all those  
5 together, that's when it became an intolerable level, and we  
6 felt that we had to complete the card swap.

7 Q So was a card swap decision made because of the post  
8 that was made and what happened after that, or is it because  
9 of free-to-air itself?

10 A It was made because of the post. At that point, we  
11 knew we had no more secret element in the system, and we  
12 knew that we were eventually going to have replace that with  
13 something that the pirates didn't know about. We actually  
14 started that process in 2001 to start placing the new Aladin  
15 card system into our new manufactured boxes, and we knew at  
16 some point we were going to have to replace all the cards.  
17 We just didn't know what the timing of that would be.

18 Q Before you began introducing a new card into the field,  
19 did you have to go through R&D and manufacturing?

20 A Yes. First NagraVision had to design the new card and  
21 design the new systems that would be used at the uplink  
22 center. This system was in parallel to the existing ROM 2,  
23 3, 10, and 11 system. So they had to design all of those,  
24 and then we had to write code for our newly manufactured  
25 set-top-boxes to be able to place this Aladin card in those

SHARON SEFFENS, U.S. COURT REPORTER

♀

7

15:34:22 1 new boxes, and we had to test the whole system out to make  
2 sure that we could authorize customers to receive  
3 programming and that everything was working properly.

4 Q How long a lead time was there?

5 A That was about two years from when we started the  
6 process to where we were able to authorize the first  
7 customer using an Aladin card on the system.

8 Q So if the evidence in this case has been that you began  
9 putting the Aladin card into the stream in June 2003, would  
10 that mean that your lead time took you all the way back to

11 possibly 2001?

12 A Yes.

13 Q When did you first become aware if there was any  
14 free-to-air problem?

15 A I believe it was in the 2003 time frame.

16 Q So you began developing this Aladin card that was going  
17 to be deployed because of the ROM 3 hack -- you started  
18 developing that before you even learned of the free-to-air  
19 problem?

20 A Yes. We knew that we no longer had a secret element,  
21 and we knew we were going to have to do a replacement  
22 eventually.

23 Q Did free-to-air give everybody the secret element, or  
24 was it the Nipper post?

25 A It was the Nipper post that did that.

SHARON SEFFENS, U.S. COURT REPORTER

♀

8

15:35:36 1 Q Now, one of the things that NDS has talked about in  
2 this case has been something called box keys.

3 Are you familiar with the term "box keys"?

4 A Yes.

5 Q If we talk about hacking, what is more important for a  
6 hacker to have, the secret keys in the Nipper post or a box  
7 key?

8 A That would be the secret keys in the Nipper post  
9 because that would actually allow you to decrypt the signals  
10 off of the satellite. The box keys were merely an ability  
11 to encrypt the messages between the Smart Card and the  
12 set-top-box. So once the Smart Card had determined what you  
13 needed to decrypt the satellite signal, that information was  
14 passed in an encrypted form to the box using the box key,  
15 but if you didn't have the keys that were in the secret  
16 element, the Smart Card, which was provided after the Nipper  
17 post, then you wouldn't have been able to decrypt the  
18 satellite signal at all.

19 Q Without the keys to the card that's found in the Nipper  
20 post, is the box key enough to reprogram an access card?

21 A No. The box key had nothing really to do with  
22 programming the access card. Again, it just allowed for the  
23 message decryption between Smart Cards and the box.

24 Q Another topic that we have talked about that the jury  
25 has heard is this posting on an FTP site of certain keys by

SHARON SEFFENS, U.S. COURT REPORTER

♀

9

15:37:05 1 Echostar. I want to focus you on that.

2 Are you aware of any type of key that was posted by  
3 Echostar on an FTP site?

4 A The only thing that I was aware that was posted on an  
5 FTP site was some of the set-top-box code when we were  
6 trying to debug a problem with one of our silicon vendors.  
7 That code was placed on an FTP, which is a file transfer  
8 protocol site, that they were able to pick up and then use  
9 us to help debug that problem.

10 There was an algorithm on there that had the location  
11 ID that we used to try to confront people that would be  
12 doing the account packing. So our group would call them up  
13 and ask them, well, if your receivers are in the house,  
14 please tell us the location ID of all your receivers. You  
15 would turn on your television set, and you could go to a  
16 screen. They would give a location ID, and there was an  
17 algorithm for that that the person at the call center could  
18 then verify that they were in front of each of those  
19 receivers.

20 If the customer couldn't do that, then they would say,  
21 well, those receivers really aren't in your household are  
22 they and try to get them to admit that they had separated  
23 the receivers and were doing account packing.

24 Q Now, if we talk about this box code that was posted on  
25 the FTP site, does that allow somebody to reprogram an

SHARON SEFFENS, U.S. COURT REPORTER

♀

15:38:38 1 access card?

2 A No. Again, it was just the set-top-box code. It had  
3 nothing to do with the code that was in the Smart Card.

4 Q So what is the linchpin, so to speak, of hacking  
5 Echostar access cards? would it be the Nipper post or the  
6 box code post?

7 A It would be the Nipper post.

8 Q Now, were you involved in trying to combat piracy after  
9 the Nipper post?

10 A Yes, I was.

11 Q what were some of the things that you did or your group  
12 did?

13 A well, I chaired a weekly meeting with a group that  
14 included some of the set-top-box hardware people/software  
15 people, the signal integrity people that were monitoring the  
16 chat rooms, some of the people from NagraStar, and sometimes  
17 we had NagraVision people in that meeting. We would get  
18 together and discuss what the status of piracy was, what the  
19 pirates had learned, what they were trying to accomplish,  
20 and how they were trying to pirate the system.

21 Then we would try to come up with electronic  
22 countermeasures that would help to keep piracy difficult.  
23 We knew we probably couldn't eliminate it at that point. We  
24 were just trying to make it difficult enough that the normal  
25 person wouldn't find it attractive, that if their

SHARON SEFFENS, U.S. COURT REPORTER

♀

15:40:10 1 programming was going down often enough they would think it  
2 was too much of a hassle, or if they had to open the box and  
3 solder wires on it that they would think that was too much  
4 of a hassle. So we were just trying to keep it at a low  
5 enough level that it wouldn't become popular.

6 Q We have heard some testimony in this case about



7 something called a patch. Are you familiar with patches?

8 A Yes.

9 Q Could you tell the jury briefly what a patch is?

10 A Well, as the patch relates to the Smart Card -- the  
11 Smart Card was manufactured with ROM code in it that was put  
12 in at manufacturing time. That's the code that the  
13 microprocessor would run. You can't change the ROM code.  
14 So if you wanted to make changes to what the microprocessor  
15 would do, you would apply a patch, and the patch would go  
16 into a writable portion of memory called the EEPROM. This  
17 patch then would change the operation, and the  
18 microprocessor then would be instructed to run that patch  
19 instead of some of the original code.

20 Q Are you aware of a patch that was deployed in early  
21 2001?

22 A Yes. Once the code became available on the Internet,  
23 we at NagraVision were able to analyze that and determine  
24 how they were modifying these Smart Cards with a buffer  
25 overflow capability where they fed way too much information

SHARON SEFFENS, U.S. COURT REPORTER

♀

12

15:41:44 1 into the card than what it expected, and then they were able  
2 to gain access to the card and be able to dump its ROM code,  
3 its EEPROM code, and also modify the Smart Card by putting  
4 blockers and things on it.

5 Q Did this patch that was sent down -- did that fix the  
6 piracy problems that resulted from the Nipper post?

7 A Well, when we did the patch, it was to fix this buffer  
8 overflow problem. It did that on cards that were in the  
9 stream at the time, but there were a lot of cards that  
10 wouldn't be in the stream that were within the manufacturing  
11 pipeline. So we were building boxes, and they would be in  
12 warehouses or in distribution or at our dealers, and they  
13 were still in the box and hadn't been installed in a  
14 customer's house yet. Those Smart Cards would have never

April 30, 2008 Volume 4 Kummer Hasak.txt  
15 received the patch, so they were still susceptible to this  
16 buffer overflow problem.

17 Then there were other cards that had been at customers'  
18 houses that had been subscribers before but were no longer a  
19 subscriber, so they had removed their satellite receiver and  
20 put it on the shelf. Obviously they weren't receiving the  
21 satellite stream, so they weren't receiving the patch as  
22 well. Then also there were cards that hackers had that had  
23 blockers put on, and they wouldn't be able to receive this  
24 patch either.

25 So there were a lot of cards in that time frame --

SHARON SEFFENS, U.S. COURT REPORTER

‡

13

15:43:30 1 somewhere around 200,000 cards -- that would still be  
2 available to use for this buffer overflow.

3 Q So it wasn't just one or two cards that were left out  
4 that weren't affected by the patch?

5 A That's correct.

6 Q Have you ever heard the phrase "close the hole" before?

7 A Yes.

8 Q And what does that mean?

9 A Well, for me, close the hole would be close whatever  
10 susceptibility the Smart Card had to being modified. So the  
11 first patch was for this buffer overflow, and we closed that  
12 hole again for the cards that received the patch. Then  
13 those cards were not available to the pirates to be modified  
14 using that technique. That meant their supply of cards that  
15 were available to them shrunk, and it was more difficult for  
16 them to find cards that hadn't had the patch applied, and  
17 then the hole was closed, that they wouldn't be able to use  
18 that particular technique, but they could use other  
19 techniques to gain access to those cards.

20 Q What does it mean for a hole to be reopened?

21 A Well, if we closed a particular card using, for  
22 instance, buffer overflow, then they could use another  
23 technique to get into the card, for instance, glitching, so

24 then there would be essentially a new hole that was then  
25 opened, and as they moved from the buffer overflow to

SHARON SEFFENS, U.S. COURT REPORTER

14

15:45:11 1 glitching, that then provided them a lot more cards that  
2 they could modify and give to their customers.

3 Q Following the buffer overflow patch, was there a  
4 significant number of ROM 3 cards still out in the field  
5 with the hole that was still open?

6 A Yes. Those were the ones that we talked about that  
7 were in the manufacturing process or they hadn't been in the  
8 stream because the customer had put it on the shelf or they  
9 had blocker codes.

10 Q Now, you haven't been here for the testimony, but there  
11 is an Exhibit 1270, which is an internal marketing document  
12 of NDS. It references that in approximately May 2001 there  
13 was in excess of 100,000 pirate devices that could be used  
14 against Echostar.

15 Do you have any reason to dispute NDS's own internal  
16 figure?

17 A No, I don't. I felt that it might have been more than  
18 that. It could be as much as a million devices, but, again,  
19 those were guesses on our part. I would say 100,000 might  
20 be low.

21 Q If we talk about the time frame of the Nipper post in  
22 December of 2000 and after you had your initial patch, did  
23 piracy expand, or were you able to control it?

24 A The piracy expanded greatly after that because there  
25 was a lot more people working on it. They had all the

SHARON SEFFENS, U.S. COURT REPORTER

15

15:46:38 1 secrets to the system. So that was a time frame when a lot  
2 more pirate devices started to -- that's when they went from

3 just using modified Smart Cards to using, for instance,  
4 emulators, connecting up PCs to set-top-boxes to look like  
5 an emulator, and also eventually doing the free-to-air  
6 boxes.

7 Q I want to focus right now on the card swap itself.

8 Have you ever heard the terms "soft swap" and "hard  
9 swap" before?

10 A Yes.

11 Q What is a soft swap?

12 A A soft swap was where we started to put these new  
13 cards, the Aladin cards, into newly manufactured boxes.  
14 Since we knew we had a problem with the old cards, we knew  
15 we had to get a new secure element in the system that the  
16 pirates didn't have access to, that they didn't know what  
17 the secrets were inside of it, so the soft swap was where we  
18 started to manufacture new boxes using that new card.

19 Then the hard swap was when we finally decided that the  
20 piracy had reached a level that had become intolerable and  
21 that we had to then send the cards to our existing customers  
22 and have them replace their old ROM 2, 3, 10 or 11 cards  
23 with these new cards. We wanted to put that off as far as  
24 possible because of the expense to do that and the hassle  
25 for our customers.

SHARON SEFFENS, U.S. COURT REPORTER

♀

16

15:48:17 1 Q Now, why didn't you immediately begin performing the  
2 soft swap right after the December 2000 Nipper post?

3 A Well, again, we thought that we could keep the piracy  
4 to a low level using these electronic countermeasures, and  
5 because we knew it was going to be expensive to provide  
6 these cards to our customers and it was also going to be a  
7 hassle for them to have to take out their old card and put  
8 this the new card -- we had it to where you had to put a  
9 particular card that you got in the mail in the correct  
10 system. If you didn't do that, then things wouldn't work

11 properly. We knew that would be a hassle for our customers,  
12 so we didn't want to undertake that until things got bad  
13 enough, and we thought we could keep it under control with  
14 these electronic countermeasures.

15 Q Would Echostar have spent \$90 million on this card swap  
16 if the buffer overflow patch was effective?

17 A No, they would not.

18 Q We have talked about ECMs. That's different than a  
19 patch?

20 A Yes.

21 Q Could you tell us a little bit about an ECM in your  
22 view?

23 A Well, ECM stands for electronic countermeasure, and  
24 there were many of those that we deployed. Some of them  
25 were targeted to the cards. Some of them were targeted to

SHARON SEFFENS, U.S. COURT REPORTER

♀

17

15:49:43 1 the set-top-boxes, and some were a combination. They were  
2 typically done to try to bring -- they were targeted to a  
3 certain set of piracy devices, and they were intended to  
4 bring those devices down.

5 Sometimes they could loop the card and make them where  
6 they were unusable again, although the pirates did find ways  
7 to unloop cards, but initially we were able to loop some of  
8 them, and some of them we were able to mark their  
9 set-top-boxes to where we could determine that they had a  
10 piracy device in.

11 what we found was some pirates kept a low level of  
12 programming with a legitimate card. They might buy like a  
13 \$20 low-end tier of programming, and then when we would do a  
14 countermeasure and take them down so that they would have  
15 some television, they would simply take out the pirate  
16 device and put their legitimate card in, and they would  
17 watch TV until the pirates got them a fix for that  
18 countermeasure that we had done.

19 So at some point, we started marking the set-top-box

20 that -- you had a pirate device in here, so even when you  
21 put a legitimate card in, we wouldn't allow that box to  
22 operate anymore, so there were a lot of different  
23 countermeasures.

24 Q Could the hacker community take certain steps to  
25 prevent the effectiveness of either the patches or the ECMS?

SHARON SEFFENS, U.S. COURT REPORTER

18

15:51:19 1 A They did take steps to do that. They would monitor  
2 what we would do, and they would determine what we had done  
3 and come up with fixes for those. Sometimes they could do  
4 that within a day, and sometimes they might last a week, so  
5 it was with different varying affects as to how long our  
6 countermeasures would last before they would respond to them  
7 and have a fix.

8 Q These patches and ECMS -- once you put a patch in a  
9 stream, does it stay there for all time?

10 A No. Eventually we are going to remove that patch. For  
11 instance, after we removed all the ROM 2, 3, 10, and 11 from  
12 the field, we no longer needed to put any of those patches  
13 out.

14 Q How about ECMS? Do they stay in the stream forever?

15 A No. We only had an ability to put a finite number of  
16 ECMS up at a time. We would typically launch an ECM. It  
17 might be up for a while. Then we would take that down.  
18 Sometimes we would rerun ECMS if we thought the pirates had  
19 rolled their devices back to an earlier level. We might  
20 relaunch an ECM, but they only had a finite period of time  
21 where they were active.

22 Q Can piracy get to the point where it's so widespread  
23 that there is not enough room in the stream to put forth all  
24 the ECMS and all the patches that you would need to combat  
25 all the types of piracy, or does piracy overrun that stream?

SHARON SEFFENS, U.S. COURT REPORTER

15:53:04 1 A We only had a finite amount of area in patches and ECMs  
2 that we could put up, so we sometimes had to take some down  
3 to put new ones up. Like I said, the pirates would  
4 sometimes roll back, but they knew that if they did that and  
5 we found there was a lot of devices using that old patch  
6 that we would just resurrect that ECM.

7 Q If you could turn to Exhibit 812, Mr. Snyder discussed  
8 that with you. Do you have that in front of you?

9 A Yes.

10 Q I want to focus -- going down about halfway, do you see  
11 the e-mail from Mr. Dugan?

12 A Yes.

13 Q In there, he says, "I do not want the card patch  
14 released due to the security leak."

15 I want you to focus on the description of security  
16 leak. Are you with me?

17 A Yes.

18 Q Does that security leak that Mr. Dugan is  
19 referencing -- does that have anything to do with the  
20 security leak with the card provider Nagra?

21 A No, I don't believe so. I think in this time frame --  
22 we had to alert our call center when we were going to do  
23 some of these countermeasures because they were going to get  
24 calls sometimes from legitimate customers because of  
25 glitches but sometimes from the pirates themselves. We had

SHARON SEFFENS, U.S. COURT REPORTER

♀

15:54:31 1 to alert them of that.

2 I believe this is referring to the fact that if we told  
3 them ahead of time we knew that some of our call center  
4 people were alerting the pirates that a particular  
5 countermeasure might be coming on a certain time or day.

6 Q So that just references the security measure that you

April 30, 2008 Volume 4 Kummer Hasak.txt  
7 were trying to put in place to make sure that your patches  
8 were more effective?

9 A Yes. It was just really a leak of the timing of when  
10 we were going to launch these countermeasures.

11 Q So it wasn't a leak of any secret keys or codes?

12 A I don't believe so, no.

13 Q Has Echostar or NagraStar to the extent you know  
14 engaged in any reverse engineering or piracy of any  
15 competitor's conditional access system?

16 A No, not that I am aware of.

17 Q Are you aware of any Echostar employee or NagraStar  
18 employee posting any proprietary information that belongs to  
19 another competitor?

20 A No.

21 Q Do you have any knowledge of any stolen documents?

22 A No.

23 MR. WELCH: No further questions, Your Honor.

24 THE COURT: Redirect by Mr. Snyder for NDS.

25 REDIRECT EXAMINATION

SHARON SEFFENS, U.S. COURT REPORTER

♀

21

15:55:47 1 BY MR. SNYDER:

2 Q Mr. Kummer, it's your testimony that the decision to  
3 make a card swap in 2002 was the result of the Nipper post?

4 A Ultimately, the Nipper post gave out all of the secrets  
5 from the Smart Card, and we knew that at some point we were  
6 going to have to do a card swap.

7 Q well, you knew when you put cards in the field that you  
8 would eventually have to do a card swap; isn't that true?

9 A We knew that --

10 Q It's not a hard question. It's yes or no.

11 You knew when you put Smart Cards in the field you  
12 would have to do a card swap eventually; isn't that right?

13 A Yes.

14 Q No Smart Card in history has ever lasted forever; isn't  
15 that right?



16 A As far as I know, that's correct.  
17 Q In fact, Smart Cards typically have a life of three or  
18 four or sometimes five years; isn't that true?  
19 A I don't know what all the lifetimes of the different  
20 cards are.  
21 Q But you know that when you start with a Smart Card  
22 eventually you are going to have to replace it if you want  
23 to stay in business; isn't that right?  
24 A If the card gets hacked, you have to replace it, yes.  
25 Q And you know that cards are eventually going to be

SHARON SEFFENS, U.S. COURT REPORTER

♀

22

15:57:28 1 hacked; isn't that true?  
2 A It's highly likely they will be hacked, but I don't  
3 think that's a foregone conclusion.  
4 Q The ROM 2 card was put in the field before the ROM 3  
5 card, correct?  
6 A Correct.  
7 Q And it was hacked, correct?  
8 A The ROM 2 was hacked, yes.  
9 Q At the point that the ROM 2 card was hacked, did  
10 Echostar know that it was inevitable that it would have to  
11 do a card swap?  
12 A At some point, we knew we would have to do a card swap,  
13 yes.  
14 Q That's not my question. You testified that the  
15 NipperClause posting made a card swap inevitable. I want to  
16 make sure the jury understands the full context of that  
17 statement.  
18 When the ROM 2 card was hacked, did Echostar know that  
19 a card swap would be inevitable?  
20 A When you say inevitable, that includes all time. You  
21 know, is it going to last 99 years? Probably not.  
22 Q I am using your words. In response to your attorney's  
23 questions, you repeatedly said because of the NipperClause

April 30, 2008 Volume 4 Kummer Hasak.txt  
24 posting you knew that a card swap was inevitable.

25 My question to you is when the ROM 2 card was hacked

SHARON SEFFENS, U.S. COURT REPORTER

♀

23

15:58:42 1 did you know then that a card swap was inevitable?

2 A We didn't think it would be within a short period of  
3 time I guess would be my answer.

4 Q My question is did you know it would be inevitable?

5 A Well, I already said that we knew when we deployed a  
6 card that it's highly likely that it is going to be hacked,  
7 and it's inevitable, so what we are arguing about is the  
8 time frame of inevitably.

9 Q When the NipperClause posting came out, Echostar  
10 already knew that a card swap was inevitable? It was just a  
11 matter of timing; isn't that right?

12 A Yes, it's always a matter of timing.

13 Q It's always a matter of timing, correct?

14 A Correct.

15 Q Now, we have seen lots of different NipperClause  
16 postings.

17 When you say the NipperClause posting made a Smart Card  
18 swap inevitable, which one are you referring to?

19 A I am referring to the one in December 2000 where it  
20 allowed the hackers to gain access to all the ROM code and  
21 eventually all the EEPROM.

22 Q So it's your testimony that there was a NipperClause  
23 posting in December 2000 that allowed access to the ROM  
24 code?

25 A Yes.

SHARON SEFFENS, U.S. COURT REPORTER

♀

24

15:59:56 1 Q Are you certain of that?

2 A Yes.

3 Q Did you see a copy of that posting?

4 A I did not.

5 Q So this posting was so important that it allowed access  
6 to the entire Echostar ROM code, and it was not sent to the  
7 person who was responsible for the anti-piracy function at  
8 Echostar; is that right?

9 A I was told about it, and I believe the people who told  
10 me, but I did not look at it myself.

11 Q Did somebody send you a memo about it?

12 A They may have. I do not recall.

13 Q We haven't seen any memos that identify any  
14 NipperClause posting as being able to dump the ROM portion  
15 of the card, so if you remember one, that would be  
16 important.

17 Did you get a memo about this Nipper posting that made  
18 a card swap inevitable?

19 A I do not remember a specific memo.

20 Q Do you remember somebody telling you that there was  
21 some posting that allowed the dumping of the ROM portion of  
22 the card?

23 A Yes.

24 Q Now, we saw during your testimony that in 1999 Echostar  
25 demanded a card swap from its card supplier Kudelski,

SHARON SEFFENS, U.S. COURT REPORTER

♀

25

16:01:08 1 Exhibit 828. Do you recall that?

2 A Yes.

3 Q Given the significance of the NipperClause posting, was  
4 there a letter demanding a card swap to Kudelski after those  
5 postings?

6 A I don't know.

7 Q You have never seen such a letter have you?

8 A I have seen letters that ask for card swaps, but I  
9 don't remember specifically when.

10 Q And you don't remember a single one that mentions a  
11 posting in December 2000 do you?

12 A Like I said, I don't remember when and what the content  
13 of that would be other than requesting a card swap.

14 Q Mr. Kummer, we also saw that in the March 2000 annual  
15 report of Echostar for the period ended December 1999 it  
16 alerted the American public as required by an SEC filing to  
17 the possibility of a card swap because the card had been  
18 hacked. Do you recall that?

19 A Yes.

20 Q Was there a disclosure to the American investing public  
21 after the NipperClause posting that that posting would  
22 result inevitably in a card swap?

23 A I don't remember what was in all of the 10-K reports.

24 Q If the NipperClause posting was something that Echostar  
25 recognized as inevitably requiring a card swap, don't you

SHARON SEFFENS, U.S. COURT REPORTER

♀

26

16:02:32 1 think it would be important to tell people that?

2 A I think if we had already alerted them that there was a  
3 possibility that a card swap was going to be required that  
4 that would be sufficient.

5 Q Well, in March 2000, these NipperClause postings hadn't  
6 occurred yet had they?

7 A Correct.

8 Q So if something happened -- if there were a material  
9 event such as these NipperClause postings that made a card  
10 swap inevitable, don't you think it would be important to  
11 tell people that?

12 A Again, I don't know what we told them or if that was in  
13 our 10-K reports after that or not.

14 Q My question isn't whether it was in there or not. My  
15 question is whether you think it would be important to tell  
16 people.

17 A I think it would be important to tell people that we  
18 had piracy in the system.

19 Q And if Echostar had decided that it was going to

20 require a card swap, wouldn't that be important to tell  
21 people, too?

22 A I am not an accountant. I don't know what needed to be  
23 put in the 10-K. I don't know if the cost of a card swap  
24 given our revenues was something that's required to be in a  
25 10-K or not.

SHARON SEFFENS, U.S. COURT REPORTER

♀

27

16:03:57 1 Q So you just don't know; is that right?

2 A Like I said, I am not an accountant. I don't know what  
3 the requirements -- what needed to be put into that 10-K or  
4 not.

5 Q So it was included in the report of March 2000 for the  
6 year end December 1999, but you don't know whether it needed  
7 to be included after that?

8 A I don't know what rose to a level that required it to  
9 be presented to our investing public.

10 Q Now, I believe it was your testimony that the  
11 NipperClause posting was what made free-to-air boxes  
12 available. Is that what you are saying?

13 A Ultimately, the NipperClause posting is what allowed  
14 piracy to flourish, and all kinds of devices became  
15 available. Pirates learned a lot about the system over  
16 time, so ultimately that culminated in the free-to-air  
17 boxes.

18 Q Before December 2000, there were piracy devices  
19 available?

20 A Yes.

21 Q There were piracy devices available for the ROM 2 card,  
22 correct?

23 A I believe there were some modified Smart Cards that  
24 used ROM 2, yes.

25 Q There were also piracy devices available for the ROM 3

SHARON SEFFENS, U.S. COURT REPORTER

♀

16:05:25 1 cards, correct?  
2 A Again, modified Smart Cards using ROM 3, yes.  
3 Q There were also emulation devices available?  
4 A I am not aware of emulation devices. I think there  
5 were some blocker devices available, but I am not aware that  
6 there were emulation devices at that time.  
7 Q Isn't it true that an emulation device uses its  
8 knowledge about the stream to decrypt it and can work  
9 without the Smart Card?  
10 A An emulation device is not the Smart Card itself, so  
11 it's not one of Nagra's Smart Cards that have been modified  
12 but it could take many forms. It might still be in the form  
13 factor of a Smart Card with a different microprocessor  
14 running different code. It may take the form of a paddle  
15 device with a microprocessor soldered on it, or it might be  
16 a cable to a personal computer which is acting as that  
17 emulation device.  
18 Q An emulation device does not require an original Smart  
19 Card; isn't that right?  
20 A That's correct.  
21 Q Before December 2000, there were emulation devices  
22 available for the Echostar system; isn't that true?  
23 A I don't remember that.  
24 Q You were the head of anti-piracy for Echostar at the  
25 time; isn't that right?

SHARON SEFFENS, U.S. COURT REPORTER

♀

16:06:51 1 A Yes.  
2 Q You are familiar with the EK-1 device?  
3 A There were a lot of devices. I don't remember all of  
4 them.  
5 Q The EK-1 device was a device that was used for  
6 emulating Echostar Smart Cards?  
7 A Again, I don't remember that specific device.

8 Q The EK-1 device was sold by a piracy group in Thunder  
9 Bay, Ontario, Canada?

10 A I don't remember the device, so I don't remember who  
11 sold it or anything about it.

12 Q Isn't it true, Mr. Kummer, that free-to-air piracy is  
13 based on knowledge of the ROM code?

14 A It's based on knowledge of the ROM code as well as the  
15 EEPROM and the keys that are within that secret element.

16 Q To accomplish free-to-air piracy, you actually have to  
17 have knowledge of the system ROM; isn't that true?

18 A I am not sure what you are referring to as the system  
19 ROM.

20 Q For the Smart Card.

21 A Yes.

22 Q And the NipperClause post did not cause dumping or  
23 access to the system ROM of the Smart Card?

24 A That's not what I understood. I understood that the  
25 post allowed people to actually dump the ROM code.

SHARON SEFFENS, U.S. COURT REPORTER

♀

30

16:08:14 1 Q Where do you get your understanding of the NipperClause  
2 posts?

3 A Mainly from reading the ECM reports that I got from my  
4 group.

5 Q You received an ECM report about a NipperClause posting  
6 that allowed the dumping of the ROM code?

7 A That's what I remember, yes.

8 Q Have you brought any of those with you today?

9 A I didn't bring anything, no.

10 Q Did your counsel show you any of those?

11 A I have looked at some ECM reports. I can't remember if  
12 those had -- referred to the ROM codes being dumped.

13 Q Do you recall any ECM report where somebody reports to  
14 you that a NipperClause posting allows the dumping of the  
15 system ROM?

16 A I don't remember a specific one, no. I mean, there  
17 were literally thousands of ECM reports.

18 Q There are literally thousands of them, and isn't it  
19 true that not a single one mentions that the NipperClause  
20 post can result in the dumping of the system ROM?

21 A I don't believe that's true, no.

22 Q Are you familiar with a memory access control matrix?

23 A No.

24 Q The memory access control matrix is a part of the Smart  
25 Card, designed into the Smart Card?

SHARON SEFFENS, U.S. COURT REPORTER

31

16:09:36 1 A I am not familiar with that, no.

2 Q Isn't it true that the memory control matrix actually  
3 protects access to the system ROM?

4 A I am not familiar with that level of detail of the  
5 internal workings of the Smart Card.

6 Q Therefore, you wouldn't know whether or not the memory  
7 access control matrix prevents an attack or recipe like that  
8 described in the NipperClause dot text file from gaining  
9 access to the system ROM; isn't that true?

10 A I don't know.

11 Q You don't know one way or the other?

12 A I don't know one way or the other.

13 Q One of the things you mentioned was that the  
14 NipperClause post provided knowledge of the buffer overflow  
15 vulnerability.

16 A That's my understanding, yes.

17 Q How do you get that understanding?

18 A Again, from the ECM reports and also from talking with  
19 NagraVision afterwards. That's how they were able to  
20 determine that there was a buffer overflow problem.

21 Q When was Nagra first aware that there was a buffer  
22 overflow vulnerability in the ROM 3 card?

23 A Well, my understanding is that was after the Nipper  
24 post, and they analyzed what the NipperClause post was



25 doing. Then they were able to determine that.

SHARON SEFFENS, U.S. COURT REPORTER

♀

32

16:10:55 1 Q They never advised you that the source code for the  
2 Smart Card was actually designed so that it wouldn't check  
3 for buffer overflow?

4 A No.

5 Q Nagra never told you that in early 2000 they met with  
6 ST and were told that the card had a buffer overflow  
7 vulnerability?

8 A I was never told that, no.

9 Q Nobody ever told you at Echostar that the card had a  
10 buffer overflow vulnerability?

11 A Not until after we were able to analyze this as the way  
12 that they were modifying these Smart cards.

13 Q That was the first you learned of it?

14 A That was the first I learned of it, yes.

15 Q So if Nagra knew of that before the December 2000  
16 posting, it was just information they hid from you?

17 A Possibly, yes.

18 Q Is it something you think you would want to have known?

19 A Yes.

20 Q Isn't it true, Mr. Kummer, that the ROM 10 card does  
21 not suffer from a buffer overflow vulnerability?

22 A I believe that's true because it was done after these  
23 issues had been found.

24 Q After what issues had been found?

25 A The buffer overflow issues within the ROM 2 and ROM 3.

SHARON SEFFENS, U.S. COURT REPORTER

♀

33

16:12:20 1 Q Isn't it true that the ROM 10 card was put into the  
2 field before December 2000?

3 A I don't remember when it was actually deployed.

4 Q Isn't it true that the ROM 10 card was actually put in  
5 the field in 1999?

6 A Again, I don't remember when we actually deployed that.

7 Q But it's your testimony that the ROM 10 card was  
8 developed after the buffer overflow vulnerability was known?

9 A That's what I thought, yes.

10 Q Now, if the buffer overflow vulnerability was known  
11 when the ROM 10 card was developed, would it have been  
12 prudent to issue a patch then for the ROM 2 and ROM 3 cards?

13 A Possibly.

14 Q I mean, if you know that the ROM 2 and ROM 3 cards have  
15 have this buffer overflow vulnerability, it would make sense  
16 to patch it?

17 A Possibly.

18 Q Are there some circumstances in which you wouldn't want  
19 to patch it?

20 A Yes.

21 Q What would that be?

22 A We have had some cases where we knew of  
23 vulnerabilities, but by doing a patch, you also alert the  
24 piracy community that there is a vulnerability. At some  
25 point, you may make a determination that because you found a

SHARON SEFFENS, U.S. COURT REPORTER

♀

34

16:13:37 1 problem it doesn't necessarily mean it's going to be found  
2 within the piracy community, so you may make a determination  
3 that you don't want to alert them to that particular  
4 vulnerability by doing a patch.

5 Q Mr. Kummer, was the buffer overflow vulnerability the  
6 kind of vulnerability you wouldn't want to alert pirates to  
7 by doing a patch?

8 A I don't know. We would have discussed it at the time,  
9 and we would have made a determination on that, but as I sit  
10 here today, I don't know if it would have been one of those  
11 types or not.

12 Q This is the same vulnerability that I believe you have  
13 testified the NipperClause posting exposed and made a card  
14 swap inevitable. Do I have that right?

15 A Yes.

16 Q So if the vulnerability was so important that its  
17 exposure to the public or by pirates could result inevitably  
18 in a card swap, wouldn't you want to close it before people  
19 started discovering it?

20 A Again, we would have made that determination at that  
21 time. I mean, you are applying 20/20 hindsight to it. I  
22 would say knowing what we know today that we should have  
23 done that, but at the time, we may have determined that it  
24 wasn't going to be found by the pirates, and that it might  
25 not have needed a patch.

SHARON SEFFENS, U.S. COURT REPORTER

35

16:15:07 1 Q Are you saying that Echostar decided it wasn't going to  
2 be found by the pirates or maybe that was Echostar's  
3 thinking?

4 A I am saying if we had known that the vulnerability  
5 exists we would have discussed it at the time and decided  
6 whether we wanted to patch it or not.

7 Q If NagraStar knew about the vulnerability, would you  
8 have expected them to tell you about it so that you could  
9 have that discussion?

10 A Yes.

11 Q After the patch was issued to close the buffer overflow  
12 vulnerability, I believe you testified that there were  
13 thousands of cards that didn't receive the patch; is that  
14 right?

15 A I believe it was a lot more than that. It was all the  
16 cards that were in the manufacturing process.

17 Q The cards in the manufacturing process and cards in  
18 inventory as well, right?

19 A Yes.

20 Q Now, when those cards are put into service -- somebody

21 turns on their set-top-box and puts the card in there --  
22 then the patch is delivered to those cards; isn't that  
23 right?

24 A If the patch is still in the air, yes.

25 Q When did Echostar take down the patch for closing the

SHARON SEFFENS, U.S. COURT REPORTER

♀

36

16:16:22 1 buffer overflow vulnerability?

2 A I don't know specifically.

3 Q This is vulnerability that you have just told the jury  
4 resulted inevitably in a card swap. Are you saying you took  
5 it down after a little while?

6 A I know at least we would have taken it down after we  
7 had done the card swap because then there would have been no  
8 more target devices. I don't know exactly when we took that  
9 patch off the air.

10 Q Let's make sure everybody has the chronology right.  
11 The patch we are talking about was in early 2001,  
12 correct?

13 A Correct.

14 Q And the DNAST-II steam that makes all those cards  
15 inoperable, that was at the end of the third quarter of  
16 2005?

17 A I remember 2005 but not which quarter.

18 Q So four or more years later?

19 A Yes.

20 Q Was the patch in the air for those four years?

21 A I don't know.

22 Q Now, Echostar knows that it has cards in process  
23 doesn't it? This isn't a secret?

24 A Yes.

25 Q It knows it has cards in warehouses?

SHARON SEFFENS, U.S. COURT REPORTER

♀

16:17:36 1 A Yes.

2 Q It knows it has cards at retail outlets, basically in  
3 the pipeline?

4 A Yes.

5 Q So if the patch were so important to close a  
6 vulnerability of this extent, it wouldn't take it out of the  
7 air right away and leave those cards out there would it?

8 A Like I said, the patch closed the hole which  
9 constricted the supply of Smart Cards that could be used as  
10 modified Smart Cards, but as those Smart Cards of the ROM 3s  
11 went out of production and we were moving to supplying ROM  
12 10s and ROM 11s, we knew that there weren't any ROM 3s in  
13 the pipeline anymore, and the likelihood of ROM 3s that  
14 would be in the field that haven't seen the stream would  
15 decrease over time.

16 So at some point, we make a decision that -- all we are  
17 really trying to do is restrict the supply of modified Smart  
18 Cards to the pirate community. So at some point in time,  
19 that 200,000, which was the bulk of them, these ones that  
20 were in the manufacturing pipeline and distributed -- at  
21 some point, we feel that they have been flushed out of the  
22 pipe, that most of them have been placed on the system by  
23 legitimate subscribers, and we have constricted that supply  
24 enough.

25 Another thing I might add is that the piracy community

SHARON SEFFENS, U.S. COURT REPORTER

♀

16:19:07 1 started to move away from modified Smart Cards as being the  
2 preferred hack. So at some point, if a modified Smart Card  
3 is no longer the preferred hack, there is really no reason  
4 to continue to patch those Smart Cards.

5 Q You said two really important things. Let me take them  
6 a piece at a time.

7 When you were asked questions by plaintiffs' counsel

8 and you said there were 200,000 cards in the stream that  
9 hadn't received the patch, you were referring to the time of  
10 the patch weren't you?

11 A Yes.

12 Q You weren't referring to the time when the patch was  
13 taken down were you?

14 A No. I was referring to the time that those cards --  
15 when the patch was first applied and those cards were in  
16 that pipeline.

17 Q When those cards went into service, they would  
18 automatically receive the patch, correct?

19 A Yes, if they went into service at a legitimate  
20 customer.

21 Q And Echostar in its prudence would not have stopped  
22 that patch until it decided that the number of cards in that  
23 pipeline was reduced to a minimum level; isn't that right?

24 A Correct.

25 Q Did Echostar ever repeat that patch?

SHARON SEFFENS, U.S. COURT REPORTER

♀

39

16:20:29 1 A I don't recall if we did or not.

2 Q It would be possible to repeat a patch wouldn't it?

3 A Yes.

4 Q If at some point Echostar decided that there were too  
5 many cards in the fields that had not received that patch,  
6 it could issue it again?

7 A It could, yes.

8 Q But Echostar never issued that patch again did it?

9 A I don't know if they did or they didn't.

10 Q Now, Mr. Kummer, when did Echostar first introduce the  
11 Aladin card?

12 A We first authorized them in a customer system in 2003.

13 Q When did you first deploy the Aladin card?

14 A In 2003, we started to put them into new set-top-boxes.

15 Q Isn't it true that you first deployed the Aladin card  
16 in 1999 before the ROM 2 system had been hacked?

17 A No.

18 MR. SNYDER: Your Honor, I would like permission  
19 to read to the witness his deposition on page 85, line 10,  
20 to page 86, line 13.

21 THE COURT: You may.

22 MR. SNYDER: Mr. Kummer, during your deposition  
23 were you asked this question, and did you give this answer?

24 "Q. So when did the swap occur?

25 "A. Well, we started to deploy the Aladin card,

SHARON SEFFENS, U.S. COURT REPORTER

♀

40

16:23:05 1 the version 101, I believe in 1999. So we actually started  
2 to deploy it before the ROM 2 system had been hacked, and we  
3 did that just because we wanted to put the latest card into  
4 the field. You always want to buy the best thing, right?  
5 So you want to get the best available technology to put in  
6 the field, and so we started to phase that into new  
7 receivers. So as we shipped a new receiver in 1999, we  
8 started to put this new ROM 101 card into it.

9 "I think by that time we didn't really talk about  
10 it, but we had gone from ROM 2 to ROM 3 to ROM 10 to ROM 11,  
11 so there were some other versions in there, but they had all  
12 been compromised over time. So we were replacing where we  
13 were shipping out the ROM 101s and/or 102s when they became  
14 available. I am not exactly sure when that became  
15 available.

16 "And then once we became hacked and the hack got  
17 worse and more and more hack customers came on board and the  
18 countermeasures became less effective, we decided that we  
19 needed to do a swap of the old cards in the field and get  
20 them to be new cards to try to resecure the system. I think  
21 that we started that in about 2004, I believe, was when we  
22 kind of made the decision, okay, we are going to replace all  
23 the old cards.

24 "And we started shipping cards to customers and

25 said here. April 30, 2008 Volume 4 Kummer Hasak.txt  
Here is your new card. You need to put this in

SHARON SEFFENS, U.S. COURT REPORTER

41

16:24:33 1 your system. You need to take the old card out, and if you  
2 don't, you are going to lose programming in some period of  
3 time.?

4 That was your testimony?

5 A Yes, but obviously I was wrong on that date.

6 Q When you testified under oath, you were just wrong?

7 A Again, I said I believed the date was that. That was  
8 my recollection at the time, but since then, I have gone  
9 back and looked at other things and talked to people, and  
10 the date was actually 2003.

11 Q Mr. Kummer, isn't it also true that in January of 2003  
12 the ROM 3 card was largely secure, but the ROM 2, 10, and 11  
13 cards had been compromised?

14 A The ROM 3 card may have been resecured at that point,  
15 but at that point, all the secrets were out. The other  
16 thing is that the pirates had moved on to these other  
17 devices such as emulators and --

18 Q And free-to-air.

19 A In 2003, we saw the first free-to-air I believe, yes.

20 MR. SNYDER: Could you show the witness Exhibit  
21 1670, please? I believe this is already in evidence, Your  
22 Honor.

23 BY MR. SNYDER:

24 Q Now, Mr. Kummer, to be clear, the ROM 10 card was not  
25 vulnerable to a buffer overflow attack; isn't that right?

SHARON SEFFENS, U.S. COURT REPORTER

42

16:25:59 1 A That's my understanding, yes.

2 Q And the ROM 11 card was not vulnerable to a buffer  
3 overflow attack?



4 A That's my understanding, yes.  
5 Q Is this one of the types of ECM reports that you are  
6 referring to that you would receive?  
7 A Yes, this looks like at least the correct format for  
8 some of these ECM reports.  
9 Q And this one is dated January 29, 2003?  
10 A Yes.  
11 Q If you look down in the middle of the first page where  
12 it says "Status: Original cards, DNAST-II," that's the ROM  
13 2 card?  
14 A Yes.  
15 Q "Hole open. Some cards have blocker software." Do you  
16 see that?  
17 A Yes.  
18 Q DNAST-III, that's the ROM 3 card?  
19 A Yes.  
20 Q "Hole closed. Some cards have blocker software"?  
21 A Yes.  
22 Q DNAST-10, that's the ROM 10 card?  
23 A Yes.  
24 Q "Freeware E3M with auto roll blocker code available for  
25 nonpatched cards." Do you see that?

SHARON SEFFENS, U.S. COURT REPORTER

♀

43

16:27:09 1 A Yes.  
2 Q DNAST-11, that's the ROM 11 card?  
3 A Yes.  
4 Q "Freeware E3M available for nonpatched cards." Do you  
5 see that?  
6 A Yes.  
7 Q So as of January 29, 2003, for ROM 2, the hole was  
8 open? For ROM 3, the hole was closed? For ROM 10, there  
9 were freeware E3Ms available? For Rom 11, there were  
10 freeware E3Ms available?  
11 A Correct.  
12 Q It's your testimony that by this time piracy started

13 move to other devices like free-to-air and emulators?

14 A Yes, and you can see a list of them underneath it here.

15 MR. SNYDER: No more questions.

16 THE COURT: Mr. Welch.

17 RE-CROSS-EXAMINATION

18 BY MR. WELCH:

19 Q Mr. Kummer, going back to your testimony about '99  
20 versus 2003 when you started to do the soft swap, what would  
21 be the best evidence of when you started to deploy cards in  
22 the field? would it be actual purchase orders or your '99  
23 testimony?

24 A Purchase orders would be one way that you could  
25 determine when we did it because we would start buying them

SHARON SEFFENS, U.S. COURT REPORTER

‡

44

16:28:41 1 to put into the new set-top-boxes.

2 Q So if Mr. Orban testified about purchase orders for  
3 purchasing the Aladin card, that would be a good place to  
4 look?

5 A That would be a good place to look among others.

6 Q I want to go back and talk about this hole open and  
7 hole closed.

8 As long as there is still one pirate card or one card  
9 that has not been fixed by a patch or an ECM, does that  
10 still create a problem for Echostar?

11 A Yes. They could still be able to exploit that device  
12 to look inside of it to see what the ROM was, to see what  
13 the EEPROM was, for instance.

14 Q As long as there was at least one pirate device out  
15 there, one access card that was not affected by an ECM or a  
16 patch, pirates could still use that to create new hacks?

17 A Well, after the post and they had gotten all the  
18 secrets for the secret element, they didn't really even need  
19 that anymore.

20 Q Now, we heard testimony from Mr. Kuykendall earlier.

21 He said that it was incredibly unlikely to find this buffer  
22 overflow without I think he said significant industrial  
23 means. Do you agree with that?  
24 A You would have to be able to analyze the ROM code in  
25 order to find this buffer overflow, yes, so you would have

SHARON SEFFENS, U.S. COURT REPORTER

45

16:30:37 1 to have somehow extracted the original ROM code which would  
2 be an expensive undertaking.

3 Q If the Headend Report is dated in November 1998, the  
4 Headend Report being the final report that the defendants  
5 created to commercially exploit the Echostar hack, are you  
6 aware of any dump of the ROM code at any time prior to them  
7 finalizing that report?

8 A Prior to 1998?

9 Q November of '98.

10 A No. The first ones were where we saw the phrase that  
11 had gotten on the Internet.

12 Q And that was after they prepared their commercial  
13 exploit of the hack?

14 A Yes.

15 Q Now, we talked about this ROM 10 card.

16 Did it suffer -- we have heard testimony about memory  
17 aliasing, index variables, and false checksum.

18 Was a ROM 10 card still susceptible to those type of  
19 hacks?

20 A It's my understanding it had glitch attacks and other  
21 types of attacks that it was vulnerable to. That's why we  
22 were patching it.

23 Q One of the things we talked about was how long a card  
24 can remain in the field.

25 When you first deployed the ROM 2 and ROM 3 cards, what

SHARON SEFFENS, U.S. COURT REPORTER

46

16:31:53 1 was your view of how long these cards would last? what was  
2 the lifespan?

3 A Well, in the absence of piracy, we would expect them to  
4 still be active today, so the real question is when would  
5 they be pirated? we didn't know how long they would last.  
6 Our guess in engineering was that they should last between  
7 five to ten years. That would be a reasonable lifetime for  
8 the cards. I think if we asked Charlie Ergen he said they  
9 should last forever.

10 Q In your view, did NDS's efforts -- did NDS's activities  
11 speed up the lifespan of the card or shorten the lifespan of  
12 the card?

13 A Definitely, yes.

14 MR. WELCH: No further questions.

15 THE COURT: Sir, we are going to place you on call  
16 as we are all of the other witnesses. You are in Colorado.  
17 The case is coming to close, but I am going to be cautious  
18 and tell you that you need to remain available until May 16.  
19 The case will conclude before then. Thank you very much.

20 Counsel, your next witness.

21 MR. SNYDER: The case calls Rubin Hasak.

22 would you raise your right hand.

23 RUEVEN HASAK, DEFENSE WITNESS, SWORN

24 THE COURT: Please be seated to my left here in  
25 the witness box.

SHARON SEFFENS, U.S. COURT REPORTER

♀

47

16:34:19 1 would you state your full name and spell your last  
2 name for the jury.

3 THE WITNESS: My name is Rueven Hasak, H-a-s-a-k.

4 THE COURT: Thank you very much.

5 This is direct examination by Mr. Snyder on behalf  
6 of NDS.

7 DIRECT EXAMINATION

8 BY MR. SNYDER:

9 Q Good afternoon, Mr. Hasak.  
10 A Good afternoon.  
11 Q Can you tell us your current position at NDS?  
12 A I am Senior Vice-President of worldwide Operational  
13 Security at NDS.  
14 Q Mr. Hasak, how many languages do you speak?  
15 A I speak good Hebrew, quite good English, and Russian.  
16 Q Are you comfortable testifying in English?  
17 A Yes. From time to time, I need some help.  
18 THE COURT: Most of the conversation can be  
19 carried on in English?  
20 THE WITNESS: Yes.  
21 BY MR. SNYDER:  
22 Q Mr. Hasak, you are the Senior Vice-President of  
23 worldwide Operational Security at NDS?  
24 A Yes.  
25 Q What does that mean?

SHARON SEFFENS, U.S. COURT REPORTER

♀

48

16:35:33 1 A It means that my responsibility is to care for the  
2 well-being of our intellectual and physical assets  
3 worldwide.  
4 Q Now, before we get into the details of that, Mr. Hasak,  
5 could you briefly describe your educational background?  
6 A I have a Bachelor's Degree from the Hebrew University  
7 in Jerusalem. I studied for a Master's Degree in the same  
8 university, and I graduated in the AMP course at Harvard  
9 University.  
10 Q What is the AMP course?  
11 A Advance Military Program for senior managers.  
12 Q Do you have any technical training?  
13 A No.  
14 Q After you graduated from the Hebrew University, what  
15 did you do?  
16 A I was a junior lecturer at the University, and then I

17 joined the Israeli Security Service.

18 Q How long were you with the Israeli Security Service?

19 A From 1964 to 1986.

20 Q Were there any breaks in your service in the Israeli  
21 Security Service?

22 A Yeah. In 1979, I went on legal absence, and I became  
23 the city manager of Jerusalem for three years.

24 Q What does it mean to be the city manager?

25 A A lot of travel. To run the city.

SHARON SEFFENS, U.S. COURT REPORTER

♀

49

16:36:55 1 Q Is the city manager a high position, sir?

2 A It's the highest nominated position, yes.

3 Q In other words, the highest nonelected official?

4 A Yes.

5 Q Did you then return to the Israeli Security Service?

6 A In 1981, I was offered by our then prime minister to  
7 come back and become the deputy head and later become No. 1.  
8 I mean to run the organization.

9 Q So when you returned to the Israeli Security Service,  
10 what number in the hierarchy were you?

11 A No. 2.

12 Q Did you hold that position until you left the Israeli  
13 Security Service?

14 A Yes.

15 Q When did you leave the Israeli Security Service?

16 A Officially at the end of 1986.

17 Q When did you leave the Israeli Security Service?

18 A I resigned under protest.

19 Q When you say you resigned under protest, what do you  
20 mean?

21 A There was a coverup story which I disagreed with, and I  
22 wanted my boss and other colleagues to take responsibility  
23 because they had the authority because I believe that  
24 whoever authority should take responsibility. I went to the  
25 prime minister and I resigned, and he didn't like it too

SHARON SEFFENS, U.S. COURT REPORTER

♀

50

16:38:07 1 much because of political reasons.  
2 Q Did that decision end your career?  
3 A Regretfully, yes.  
4 Q After you left the Israeli Security Service, where did  
5 you work?  
6 A I was working again with the mayor of Jerusalem,  
7 consulting with him. Then I joined my two colleagues, and  
8 in 1999, we established a security consulting company in  
9 Israel company named Shafran.  
10 Q Have you also served served in the military?  
11 A Yes.  
12 Q For how long did you serve in the military?  
13 A As a matter of fact, I serve until today as a  
14 volunteer.  
15 Q When you were you on active duty?  
16 A The last time you mean?  
17 Q For what period of time?  
18 A Three years like everybody else. I was an officer, so  
19 I had to sign for one year, and I served three years in the  
20 regular Army.  
21 Q What was your rank when you left active duty?  
22 A Major.  
23 Q But you currently volunteer now in the Reserves?  
24 A Yes, as a simple soldier.  
25 Q When you volunteer in the Armed Services, in what

SHARON SEFFENS, U.S. COURT REPORTER

♀

51

16:39:22 1 capacity is it?  
2 A As a private soldier replacing young soldiers mainly  
3 during our holidays so they can go home.  
4 Q When did you join NDS?

5 A February 1996.

6 Q Have you always held the position of head of worldwide  
7 Operational Security?

8 A Yes.

9 Q What is included in your duties as head of worldwide  
10 Operational Security?

11 A And I said before, my responsibility starts in the  
12 well-being of the physical efforts of the company, and it  
13 goes to the intellectual assets of the company. In order to  
14 keep them secured and protected, we are doing a list of  
15 things starting from simple things like developing access  
16 control through security, and it ends at anti-piracy.

17 Q So one of your functions is to fight piracy?

18 A Yes.

19 Q Does NDS fight piracy of only its own system?

20 A No. Our philosophy is that we have to fight piracy  
21 which refers to NDS and to fight worldwide piracy.

22 Q Now, you mentioned that one of the things you are  
23 responsible for is physical security?

24 A Yes.

25 Q Can you describe generally what you do to protect the

SHARON SEFFENS, U.S. COURT REPORTER

♀

52

16:40:55 1 physical assets of NDS?

2 A It starts from quite strict access control. Everyone  
3 must have a badge, locked rooms, locked cases, guarding the  
4 company, et cetera.

5 Q Are you also responsible for protecting data security  
6 at NDS?

7 A Yes, sir.

8 Q Can you describe generally and slowly what you do to  
9 protect data security at NDS?

10 A We have a team of six or seven people worldwide who are  
11 running our data security. It starts from simple things  
12 like a password, protecting the network, building the



13 firewalls, blocking any vulnerable penetration, closing any  
14 loopholes, et cetera. A couple of things are very  
15 professional, and not everything I know the details.

16 Q Does part of that effort include having employees sign  
17 confidentiality or nondisclosure agreements?

18 A Yes. Everybody who joins NDS signs these papers.

19 Q Do you also take measures to protect NDS information at  
20 customers or vendors?

21 A Yes. One of our main things is to cooperate with  
22 customers and vendors because we realize that upon needing  
23 the protection and security of our own premises pirates try  
24 to infiltrate customers and vendors. So we cooperate with  
25 our customers to have our security policy, and whenever we

SHARON SEFFENS, U.S. COURT REPORTER

♀

53

16:43:41 1 sign a contract with a vendor, there is one item which says  
2 that they should comply with our security countermeasures.

3 Q Now, in addition to protecting physical assets and  
4 information assets, does NDS do other things to fight  
5 piracy?

6 A Absolutely, yes. It's not enough to have just a  
7 defense. You have to be proactive, and we are taking all  
8 kinds of proactive measures in order to fight piracy.

9 Q Can you describe very generally the types of measures  
10 that you take in the NDS Operational Security Department to  
11 fight piracy?

12 A In order to be able to fight piracy in an effective  
13 way, you must have intelligence. Intelligence is a key  
14 point in order to build the security system to prevent  
15 pirates from breaking our system, so the basic thing I think  
16 is getting intelligence.

17 Q Can you describe very generally the different ways that  
18 NDS collects intelligence?

19 A Yeah. There are two, three, four ways. One is  
20 monitoring the Internet. We are monitoring the Internet in  
21 more than 20 relevant languages. We record agents. We

22 employ informants, and we get information from law agencies  
23 when it is relevant and from international anti-piracy  
24 organizations.

25 Q Now, one of things that you mentioned, Mr. Hasak, was

SHARON SEFFENS, U.S. COURT REPORTER

54

16:45:34 1 recruiting agents.

2 what do you mean by an agent?

3 A An agent is an ex-pirate who was recorded by us, and he  
4 is being handled, activated, to stay in the pirate community  
5 and give us relevant information.

6 Q Was Chris Tarnovsky an agent for NDS?

7 A Yes.

8 Q How many agents does NDS have now of the type you just  
9 described?

10 A Two or three.

11 Q What is the most agents that NDS has ever had?

12 A Four.

13 Q So it's relatively rare?

14 A Oh, yeah. It's a big operation, yeah.

15 Q Now, you also mentioned that NDS uses informants?

16 A Yes.

17 Q What do you mean by informants?

18 A An informer is a person who is close to the pirate  
19 community, and he tells us whatever information he gets from  
20 from these places, but he is not activated. He is not  
21 handled.

22 Q What is the difference in information flow between an  
23 agent and an informant?

24 A An agent gets an assignment. We share with him  
25 information, and he is quite a close member of the relevant

SHARON SEFFENS, U.S. COURT REPORTER

55

16:47:14 1 people on the team.

2 Q How do you decide whether or not someone is suitable to  
3 be an agent?

4 A First of all, he should have the capability. By  
5 capability, I mean he should be very knowledgeable. He  
6 should be I would say a star, top of the art. So he has the  
7 capability to know and to get information and to talk to  
8 other pirates and be able to feed us with a pirate way of  
9 thinking and of operating. So if has the capability, we try  
10 to find out about his character. Is he the character that  
11 would be suitable to us? Is he going to be loyal, and what  
12 would be his benefit to us?

13 Q When you say his character, what are you referring to?

14 A We don't take somebody that has a criminal record. We  
15 don't take somebody who is connected to heavy criminals. He  
16 should be one that thinks working with NDS is a good  
17 opportunity for him; that he has family, relatively young so  
18 he can build his future with a respectable family; that he  
19 doesn't have any strange ideas or something like that; that  
20 though he is a hacker or a pirate, still he can play in a  
21 box, in a square.

22 Q By in a box, do you mean play by the rules?

23 A Play by the rules, exactly, yes.

24 Q Do you use agents at times for operations?

25 A Yes.

SHARON SEFFENS, U.S. COURT REPORTER

♀

56

16:49:18 1 Q As part of your operations, do you ever use competitor  
2 information?

3 A No.

4 Q Would you ever allow such a thing?

5 A No.

6 Q If someone were going to do an operation involving  
7 competitor information at NDS, would you have to know about  
8 it?

9 A It's a very theoretical question, but the answer is  
10 yes.

11 Q And you have never approved any such operation?

12 A No.

13 Q Now, do you sometimes use customer information in  
14 operations?

15 A Yes.

16 Q Do you always get the customer's permission before you  
17 do an operation that involves customer information?

18 A Yes.

19 Q Can you think of any examples of operations that you  
20 have run using customer information?

21 A Yes. We had an operation against pirates in Canada.  
22 It was a team of Ron Ereiser, and we were going to supply  
23 them with that DirectTV software in order to build the  
24 reputation of our agent. Before we did it, we got the  
25 approval from DirectTV.

SHARON SEFFENS, U.S. COURT REPORTER

♀

57

16:50:40 1 Q Who was the agent whose reputation you were building?

2 A Chris Tarnovsky.

3 Q Now, Mr. Hasak, we will come back to that, and I will  
4 show you some documents from that operation.

5 You also mentioned that you cooperate with law  
6 enforcement.

7 A Yes.

8 A Yes, sir.

9 Q Can you give the jury an example of some of the work  
10 you have done cooperating with law enforcement?

11 A There are several pirates who are today in jail in the  
12 states because of us giving the law agencies intelligence or  
13 information regarding those people. A recent example is  
14 Marty Mullens who is jailed for seven years because of  
15 money-laundering, using a false passport.

16 Q As part of your operations, do you sometimes use  
17 disinformation?

18 A Yes.

19 Q What do you mean by disinformation?

20 A Disinformation means that I am trying to plant a piece  
21 of information in the head of the pirates in order to divert  
22 them to something else, to another track.

23 Q Can you give us an example of an operation that you  
24 have done using disinformation?

25 A Yes. It was in the UK. We knew that some pirates are

SHARON SEFFENS, U.S. COURT REPORTER

58

16:52:25 1 dealing with period 10 or 11 -- I don't remember -- of  
2 BskyB. We fed them information that the changeover is going  
3 to happen in two or three months when actually it was more  
4 than a year, so for them to work for a hack for two or three  
5 months is no good, so they stopped working on it.

6 Q Have you ever used Chris Tarnovsky in an operation to  
7 spread disinformation?

8 A Not like this, no. As I mentioned before, it was an  
9 operation of the software which is kind of, but no. The  
10 answer is no.

11 Q Does NDS ever spread disinformation about its  
12 competitors?

13 A You said spread?

14 Q Does NDS ever spread disinformation about its  
15 competitors?

16 A No.

17 Q Why not?

18 A Because it's against our rules. We don't do it.

19 Q Is it difficult to run operations using disinformation?

20 A Very difficult.

21 Q Why?

22 A Because in order to be smarter than them and to feed  
23 them with the information that you want to feed them, you  
24 have to give them also a piece of real information, and you  
25 have to do it very slowly. You cannot just say on the

16:53:47 1 Internet the changeover is in two months. You have to do it  
2 in a very intelligent way.

3 Q I would like to ask you a few questions about the  
4 relationship between your group, Operational Security, and  
5 some of the other departments at NDS.

6 A Yes.

7 Q Does Operational Security sometimes work with the  
8 Marketing Department?

9 A Yes.

10 Q Can you describe briefly and again slowly the  
11 relationship between your Operational security Department  
12 and the Marketing Department?

13 A Mainly in two ways. We supply them with periodical  
14 Internet research -- I mean reports. We give it to them.  
15 Sometimes it happens that they ask us to do a specific  
16 Internet report. That's one way. The other way -- from  
17 time to time, it happens that I am going to meet potential  
18 security -- potential customers, and I describe to them what  
19 operational security is.

20 Q Is there any limit on the kinds of information that you  
21 will provide from Operational Security to the Marketing  
22 Department?

23 A Only public information that they can use. I mean  
24 mostly from the Internet.

25 Q Does the Operational Security Department provide

16:55:28 1 nonpublic information to the Marketing Department?

2 A No.

3 Q Now, does NDS also have an R&D Department?

4 A Yes.

5 Q What is the relationship between your Operational  
6 Security Department and R&D?

7 A Sometimes they ask us questions to find out on the  
8 Internet answers to some technical inquiry. Sometimes we  
9 are running for them research regarding new devices. We  
10 buy -- we purchase most of the pirate devices that are in  
11 the market, and we give it to our R&D.

12 Q Are you familiar with a group called the Haifa Research  
13 Center?

14 A Yes.

15 Q That group is sometimes called the Black Hat Team?

16 A It's kind of a nickname, yes.

17 A Yes.

18 Q Have you ever received any reports or information from  
19 the Haifa Research Center or Black Hat Team?

20 A Flow.

21 Q Are you aware that the Black Hat Team or Haifa Research  
22 Center has reverse engineered cards?

23 A I know that they are running technical research I call  
24 it because I am not technical enough to understand what is  
25 research engineering, so I refer to as technical research,

SHARON SEFFENS, U.S. COURT REPORTER

‡

61

16:57:05 1 yes.

2 Q Are you aware that the Haifa Research Center has done  
3 technical research on competitor cards?

4 A Yes.

5 Q Have you ever received any information or code from the  
6 Haifa Research Center's work on competitor cards?

7 A Never.

8 Q Are you aware that the Haifa Research Center does  
9 reports on the work that it does on competitor cards?

10 A I don't know if they do reports. I never saw it.

11 Q Have you ever received a report from the Haifa Research  
12 Center of their work on a competitor card?

13 A No.

- 14 Q Have you heard of a thing called the Headend Report?  
15 A I heard of it in this lawsuit.  
16 Q Before this lawsuit, had you heard of the Headend  
17 Report?  
18 A No.  
19 Q Before this lawsuit had you ever received a copy of the  
20 Headend Report?  
21 A No.  
22 Q Did you ever receive any code or information from the  
23 Haifa Research Center regarding the technical research they  
24 did on the Echostar card?  
25 A No.

SHARON SEFFENS, U.S. COURT REPORTER

♀

62

- 16:58:12 1 Q Did anybody ever give you any code from the Echostar  
2 card to give to anybody else?  
3 A No.  
4 Q Did anybody ever give you any code to post on the  
5 Internet?  
6 A No.  
7 Q Now, Mr. Hasak, does the Haifa Research Center  
8 sometimes ask Operational Security to obtain materials for  
9 them?  
10 A Yes, a couple of years ago.  
11 Q What kinds of materials?  
12 A They asked us to get for them conditional access cards,  
13 Smart Cards.  
14 Q For what systems?  
15 A It was an Echostar system.  
16 Q And where did you get those cards?  
17 A I asked -- I mean, my people asked the team in the USA,  
18 namely, John Norris to get these cards.  
19 Q Did Mr. Norris get those cards?  
20 A Yes -- I don't know if he personally, but, yes, they  
21 got the cards.



22 Q The Haifa Research Team got the cards?

23 A Yes.

24 Q Does Operational Security provide any other services or  
25 materials to the Haifa Research Center?

SHARON SEFFENS, U.S. COURT REPORTER

♀

63

16:59:37 1 A Not that I remember, no.

2 Q Has the Operational Security Department provided other  
3 types of cards to the Haifa Research Center?

4 A Maybe supply them with other cards. I don't remember  
5 now which ones.

6 Q What is your general procedure for obtaining cards for  
7 system?

8 A Usually we used to buy it on the Internet or ask for it  
9 from a legitimate subscriber.

10 Q Now, one of the things we have heard testimony about is  
11 some trips made to the United States by Mr. Shkedy and  
12 Mr. Mordinson.

13 THE COURT: Do you want to start there tomorrow or  
14 finish -- you choose the time.

15 MR. SNYDER: Now that I introduced it, I bet  
16 people are interested. Why don't I just finish these few  
17 questions.

18 THE COURT: You choose a logical location.

19 BY MR. SNYDER:

20 Q Are you aware that Mr. Mordinson and Mr. Shkedy visited  
21 the United States as part of their work?

22 A Yes.

23 Q Did you have any involvement in those trips?

24 A Yes.

25 Q What was your involvement?

SHARON SEFFENS, U.S. COURT REPORTER

♀

64

17:00:50 1 A But you said the U.S. It was not only in the U.S.  
2 Q where else did they visit?  
3 A It was the U.S. and Canada.  
4 Q Did you have any involvement in arranging those trips?  
5 A Yes.  
6 Q what was your involvement?  
7 A I was asked to find out several people who were  
8 subscribers to the Echostar system.  
9 Q why were you asked to do that?  
10 A Because I had to find places where they can use the  
11 card for their research.  
12 Q what did they tell you about why they needed names of  
13 people who had subscriptions to Echostar?  
14 A Because they needed to be under the footprint of  
15 Echostar to run this research with the cards.  
16 Q Did they tell you anything more about what they were  
17 going to do other than it was research?  
18 A No.  
19 Q Did you ask them?  
20 A No.  
21 Q why not?  
22 A Because it was sufficient for me that it was research.  
23 It was okay for me.  
24 Q what did you find for them?  
25 A we were looking for relatives or friends of our team

SHARON SEFFENS, U.S. COURT REPORTER

♀

65

17:02:09 1 members that we can refer these two gentlemen, Shkedy and  
2 Mordinson, to them. we called three or four names that were  
3 friends or relatives of people on our team in Jerusalem.  
4 Q And how did you select those people?  
5 A Just we knew the names. I asked our team who knows  
6 somebody in the states or Canada that we can refer our  
7 friends to them, not to bother them too much but to visit  
8 them, and we got three or four names.  
9 Q when you got those names, what did you do then?

10 A I asked the relevant people on the team -- I think  
11 there were two people on the Jerusalem team that gave names.  
12 I asked them to call these people and tell them that Shkedy  
13 and Mordinson are going to visit them for a day or  
14 something, and they should host them.

15 Q Are you talking about two people on your team that you  
16 contacted?

17 A No. Two people on our team gave the names in the  
18 States and in Canada. They knew these people. They were  
19 relatives. So they called them and told them please expect  
20 a visit from Mr. Shkedy or Mr. Mordinson for one or two days  
21 and if you could please help them.

22 Q Did you then pass those names on?

23 A Yes, to Shkedy and Mordinson.

24 Q And other than giving them those names, did you have  
25 any other involvement in those trips?

SHARON SEFFENS, U.S. COURT REPORTER

♀

66

17:03:41 1 A Nothing.

2 Q Do you have any idea what they were doing on those  
3 trips other than research?

4 A I told you before Internet research. That's what I  
5 knew.

6 MR. SNYDER: Your Honor, I think this would be a  
7 good place to break.

8 THE COURT: Do not form any opinions on this case  
9 or discuss the case. We will see you tomorrow at 8:00.

10 Thank you, sir. We will see you tomorrow.

11 (Jury not present.)

12 THE COURT: Off the record.

13 (Off-the-record discussion.)

14 THE COURT: Mr. Hagan is present. Mr. Eberhart is  
15 present. They are the primary attorneys arguing this motion  
16 this evening concerning the three priors regarding Mr.  
17 Maldonado.

18  
19 exclude the evidence of prior criminal convictions with a  
20 memorandum of points and authorities in support submitted by  
21 NDS, Mr. Stone and Mr. Snyder apparently being the authors.  
22 The Court up to this time of course had received no notice  
23 from Echostar concerning their intent to impeach  
24 Mr. Maldonado.  
25 Counsel, first concerning notice to the Court to

SHARON SEFFENS, U.S. COURT REPORTER

67

17:30:50 1 give the opportunity to NDS to argue impeachment, the code  
2 indicates that under Rule 609(b) the ten-year time limit  
3 from conviction or release from confinement, whichever is  
4 later -- unless the Court after notice finds the probative  
5 value substantially outweighs the prejudicial effect. Now,  
6 that notice could be argued concerning any felony with a  
7 ten-year limitation potentially. Apparently NDS has chosen  
8 to argue that notice applies to any impeaching felony, and  
9 therefore, you are precluded procedurally.

10 when did you receive notice of Mr. Maldonado of  
11 having felony priors and which felony priors?

12 MR. HAGAN: We first learned this information  
13 about Mr. Maldonado when we deposed him at the courthouse  
14 the day before yesterday.

15 THE COURT: Echostar deposed Mr. Maldonado the day  
16 before yesterday, which would be the 28th?

17 MR. HAGAN: Yes.

18 THE COURT: And that would be one of the evening  
19 sessions? It was on a Monday evening wasn't it, or was it  
20 Sunday?

21 MR. EBERHART: Monday afternoon actually.

22 THE COURT: Now, up to that time, had NDS in any  
23 written letter or notification to you informed you of those  
24 specific priors that Mr. Maldonado had?

25 MR. HAGAN: They had not.

♀

17:32:56 1 THE COURT: Let me check with Mr. Eberhart or  
2 Mr. Stone.

3 Have you anytime prior to April 28 in writing or  
4 by notice to this Court informed counsel concerning  
5 Mr. Maldonado having priors?

6 MR. EBERHART: No. We were not aware of the  
7 specifics before that time.

8 THE COURT: So everybody then became aware -- it  
9 sounds to the Court as if everybody became aware two days  
10 ago. Is that correct?

11 MR. EBERHART: I think that's fair, Your Honor,  
12 unless J.J. Gee knew which we don't know.

13 THE COURT: The notice provisions then are  
14 inapplicable.

15 So let me hear the arguments concerning these  
16 three priors. I have received NDS's motion. I have read  
17 that now twice. If you like more time to prepare or file a  
18 written motion, I would be happy to entertain that so nobody  
19 feels pushed because I just received it half an hour ago,  
20 although I think Mr. Eberhart was kind enough to inform me  
21 this morning just as we were starting that I should expect  
22 some briefing today, and I asked him to get that to me as  
23 quickly as possible.

24 Mr. Hagan.

25 MR. HAGAN: Your Honor, under 609, we believe that

SHARON SEFFENS, U.S. COURT REPORTER

♀

17:34:10 1 at minimum two of these crimes can come in to impeach the  
2 credibility of Mr. Maldonado. We also believe that the  
3 third crime, burglary, which is without argument outside the  
4 ten-year limitation period can still be admissible under the  
5 Court's discretion if the Court determines that the

6 probative value of that conviction outweighs any prejudicial  
7 effect. The prejudicial effect, if any, is going to be  
8 negated by the fact that Mr. Maldonado has two additional  
9 felony convictions.

10 THE COURT: Well, it's not probative value  
11 outweighs. It's substantially outweighs.

12 MR. HAGAN: Substantially outweighs. The  
13 prejudicial effect of impeaching a witness' credibility with  
14 the conviction of a felony is that the jury believes, well,  
15 he is a bad guy. We shouldn't take his word for it when he  
16 takes the stand to testify to X, Y, and Z.

17 That prejudicial effect is negated in this  
18 particular instance because Mr. Maldonado has two additional  
19 felony convictions within the ten-year limitation period, so  
20 his credibility is going to be impeached --

21 THE COURT: Which are?

22 MR. HAGAN: In 2003 --

23 THE COURT: So in other words, what you are saying  
24 is Mr. Maldonado didn't even make the ten-year limitation  
25 from 1991, and the Court should not look back from 2008 and

SHARON SEFFENS, U.S. COURT REPORTER

♀

70

17:35:38 1 extend a ten-year limitation?

2 MR. HAGAN: That's correct. I think that his  
3 criminal record shows a pattern and practice of felonious  
4 conduct which the jury should certainly be apprised of  
5 before assessing the credibility and weight to be given to  
6 his testimony under oath.

7 THE COURT: Mr. Eberhart.

8 MR. EBERHART: With respect to the burglary  
9 conviction, there is absolutely no probative value of that  
10 conviction. It has no bearing on the testimony that  
11 Mr. Maldonado is expected to give. The rule is quite clear  
12 that if it's outside the ten-year window it is subject to  
13 the Court's discretion on being admitted, and to admit it

14 the Court must find that the probative value substantially  
15 outweighs the prejudicial effect.

16 Nor do we agree that the fact that Mr. Maldonado  
17 has additional felony convictions takes away the sting of  
18 the burglary conviction as Mr. Hagan -- in fact, I think the  
19 additional convictions compound the sting of the earlier  
20 conviction for burglary. So we believe that the prejudicial  
21 effect is substantial, and that conviction should be kept  
22 out.

23 The other two convictions are a separate issue,  
24 and I presume the Court is going to address those in a  
25 minute.

SHARON SEFFENS, U.S. COURT REPORTER

♀

71

17:37:02 1 THE COURT: I want all of the priors addressed by  
2 all of you, and then I am going to make a ruling.

3 MR. EBERHART: On the other two priors, the  
4 attempted fraudulent schemes and artifices -- we concur the  
5 fact of that conviction comes in under Rule 609. However,  
6 the attendant facts and circumstances should be excluded.

7 The particular concern here is that the attendant  
8 facts and circumstances that plaintiffs will attempt to  
9 introduce are the other conviction that he was -- that he  
10 had from the same arrest. That was a conviction for  
11 attempted child exploitation. That conviction we believe  
12 must be excluded under Rule 403. It has no bearing  
13 whatsoever on his testimony that he will give. His  
14 testimony relates to his involvement in satellite piracy.

15 THE COURT: Anything further?

16 If not, I will turn back to Echostar. Mr. Hagan.

17 MR. HAGAN: Yes, Your Honor, with respect to the  
18 child exploitation and the fraudulent schemes, those felony  
19 convictions are from 2003, and they certainly come in to  
20 impune the credibility of Mr. Maldonado.

21 The burglary conviction while outside the ten-year  
22 rule is still more probative than prejudicial and

23 substantially more so because it establishes a pattern and  
24 practice that this gentleman is willing to engage in  
25 unlawful criminal acts with utter disregard to the laws of

SHARON SEFFENS, U.S. COURT REPORTER

72

17:38:58 1 the United States.

2           The jury needs to be able to assess his  
3 credibility, and it's particularly true in this instance  
4 because Mr. Maldonado will be asking the jury and the  
5 defendants through the testimony of Mr. Maldonado to take  
6 his word for certain evidentiary points. Mr. Maldonado does  
7 not have nor has he produced to us any documentation that  
8 supports his testimony that would link credibility to his  
9 testimony, so in reality he is just asking the jury to take  
10 his word for it.

11           They are certainly entitled to consider the  
12 pattern and practice of felony conduct that Mr. Maldonado  
13 has engaged in as well as any agreements he may have reached  
14 with the defendants in this case to determine how much  
15 weight they need to give to his testimony.

16           THE COURT: Anything further? This will be the  
17 last round.

18           MR. EBERHART: With respect to the issue of  
19 whether Mr. Maldonado has produced any proof to support his  
20 testimony, he has produced such proof. He has produced and  
21 we have provided to the plaintiff several weeks ago a wire  
22 transfer that shows monies he transferred to Barrie,  
23 Ontario, to pay for piracy devices.

24           His testimony is also supported by the written  
25 documentation of J.J. Gee and the testimony of J.J. Gee that

SHARON SEFFENS, U.S. COURT REPORTER

73

17:40:16 1 was delivered to this Court. J.J. Gee raided Mr. Maldonado,



2 and Mr. Gee testified at some length about the raid and what  
3 he was told by Mr. Maldonado during that raid.

4 Mr. Maldonado's testimony is going to be largely consistent  
5 with what Mr. Gee said. They differ on a few points, but  
6 largely they have the same recollection of that meeting.

7 THE COURT: I am going to trace some of the  
8 history not only in the federal courts but also the state  
9 courts because it's a fascinating history concerning priors.

10 Historically at least in California, the  
11 California courts worked with a case in the 1970s and early  
12 '80s called People versus Beagle. There four criteria were  
13 set out concerning priors.

14 One was that the crime involved moral turpitude.

15 The second was that the crime was not so same or  
16 similar to the -- the impeaching felony was not so same or  
17 similar to the substantive crime to lead a jury into what we  
18 would believe when I was practicing in the state court and a  
19 judge so many years an automatic conviction. Therefore, if  
20 you had a burglary as a substantive offense and you were  
21 impeaching with a burglary, the danger was if you allowed  
22 the burglary that the jury would assume that the gentleman  
23 or woman was involved and should be convicted of the charged  
24 crime before the Court.

25 The third was initially there was some time

SHARON SEFFENS, U.S. COURT REPORTER

74

17:41:51 1 limitation, but it was rather loose in California. It  
2 wasn't a ten-year limitation. It was somewhat of a  
3 balancing test under what we call 403 in the Federal Rules  
4 of Evidence, and the California Legislature and the courts  
5 eventually moved away from that, and now in California there  
6 are priors used for impeachment without any time limitation.

7 A balancing test can take place at the Court's  
8 discretion, but in California at least, the courts start  
9 with the presumption that all felonies if they involve moral

10 turpitude are admissible. The third was a difficult prong  
11 for California courts to gauge. So many of us labored under  
12 what I am going to call a chilling effect. Under Beagle and  
13 its progeny, the concern was was the prior a prior that  
14 would literally chill and keep usually the defendant who was  
15 on trial from testifying? We would balance that over the 17  
16 years that I was a state court judge, and the end result was  
17 almost any prior it could be argued would keep off the  
18 stand, but a multitude of priors, a cascade of priors, the  
19 same or similar priors, could have such an effect.

20 In those years, courts actually started sanitizing  
21 priors. So if you had a same or similar prior, a burglary  
22 prior and a substantive offense that was a burglary, for a  
23 while, the Court's actually would say -- allow counsel to  
24 ask is it true you have been convicted of a crime involving  
25 moral turpitude? Yes.

SHARON SEFFENS, U.S. COURT REPORTER

75

17:43:45 1 well, the California Supreme Court eventually made  
2 short work of that, and they were absolutely correct in this  
3 humble Court's opinion because when you said a crime of  
4 moral turpitude that could be murder. It could be rape. In  
5 other words, the prior itself could be worse than the  
6 sanitizing that had taken effect.

7 so the California Legislature and the courts now  
8 at least in the state of California allow priors without  
9 time limitations, and the same or similarity effect is  
10 really a 403 determination under California State Courts.  
11 The chilling effect is always chilling for anybody who is  
12 testifying, including a defendant. The extent of the moral  
13 turpitude moved to a crime involving, quote, "a readiness to  
14 do evil." That became the California standard.

15 I want to walk through with you now the federal  
16 standard. The federal standard is significantly different  
17 and interesting. In (a)(1), this allows punishment -- or  
18 impeachment of crimes punishable by death or imprisonment in

19 excess of one year. I think we can all agree that all three  
20 of these priors are in excess of one year.

21 If you notice, there is no limitation in  
22 609(a)(1). It goes onto read "are admissible to impeach a  
23 witness other than the accused subject to Rule 403, and such  
24 crimes are admissible to impeach an accused if the Court  
25 determines probative value outweighs the prejudicial effect

SHARON SEFFENS, U.S. COURT REPORTER

♀

76

17:45:16 1 to the accused."

2 (a)(1) says nothing about moral turpitude. It's  
3 almost a prior without limitation. I still think that we  
4 should be making those findings, and in a few moments for  
5 those priors that are admissible, I will make those  
6 findings.

7 Subsection (2) involves a specific type of felony  
8 crime: crimes involving dishonesty or a false statement.  
9 Well, there you have got the old moral turpitude standard in  
10 a sense or a readiness to do evil if you use the present  
11 California Supreme Court standard. So the Court really has  
12 this hybrid of almost any felony on one side and crimes  
13 involving moral turpitude or what I am going to say under  
14 the federal court are explicitly involving dishonesty or a  
15 false statement.

16 where does that leave us? Graham James did not  
17 testify, but if Graham James would have testified, this  
18 Court would have certainly allowed his impeachment for child  
19 molestation, and NDS had asked the Court to do so, had risen  
20 to the occasion, and my ruling can't be based upon my  
21 allowance of impeachment by NDS, but you both find  
22 yourselves in similar waters with the child exploitation  
23 case and with the Graham James matter. Both of those are  
24 going to come in in front of jury.

25 First of all, they are certainly within the

SHARON SEFFENS, U.S. COURT REPORTER

♀

77

17:46:56 1 ten-year period of time. No. 2, each of those crimes -- but  
2 specifically focusing on Mr. Maldonado and the 2003  
3 attempted exploitation of a minor involved not only moral  
4 turpitude, a readiness to do evil -- it is a crime  
5 involving, if you will, the moral aspects and turpitude of  
6 those moral aspects that the jury should be aware of in  
7 terms of impeachment.

8           The time limitations are not in question. It's  
9 certainly within ten years. It's not the same or similar  
10 kind of conduct that would cause a juror to be prejudiced, a  
11 burglary -- or a substantive burglary, and the chilling  
12 effect, I have no way of discerning that except that it  
13 seems like -- I probably don't have to address it. I am  
14 just so used to going through those factors on the state  
15 court level that I thought I would spend a little bit of  
16 time with them.

17           Concerning the attempted fraudulent scheme or  
18 artifice, it's interesting because if the Court had only let  
19 in the fraudulent scheme or artifice it's actually a false  
20 impression to the jury.

21           NDS -- your position is Maldonado is an  
22 accomplished person in the piracy world, and in effect, it  
23 would be to your benefit and somewhat inequitable to allow  
24 one prior to come in when it's supposed to be for moral  
25 turpitude reasons for impeachment purposes because it

SHARON SEFFENS, U.S. COURT REPORTER

♀

78

17:48:44 1 actually bolsters your case. You want him to appear like a  
2 pirate. You want him to be part of the community. You  
3 actually want him to be going up to Barrie, Ontario, and  
4 purchasing devices or part of this scheme or the potential  
5 pirate. I think it gives a false impression of who the

April 30, 2008 Volume 4 Kummer Hasak.txt  
6 gentleman is.

7 This fraudulent scheme or artifice has the aspects  
8 of moral turpitude. It is not a concern concerning time  
9 limitation, being within ten years. It is not the same or  
10 similar effect, but if it is, it is still absolutely  
11 relevant, and the probative value outweighs the prejudicial  
12 effect.

13 Finally, the chilling effect is just a hard  
14 criteria to address. Any witness can claim that they are  
15 chilled in this manner. I don't know if Mr. Maldonado will  
16 be or not, but we will see tomorrow if he testifies.

17 So it involves dishonesty. Both crimes do. The  
18 false statement certainly is the attempted fraudulent scheme  
19 or artifice. The attempted exploitation of a minor involves  
20 dishonesty.

21 Now the question becomes the burglary. What does  
22 the Court do with a 1991 burglary? Frankly, the safe call  
23 is to simply exclude that burglary. I am not going to make  
24 that call. This burglary is absolutely admissible for a  
25 number of reasons. First of all, it's a crime of moral

SHARON SEFFENS, U.S. COURT REPORTER

♀

79

17:50:13 1 turpitude. It involves a time limitation that the Court is  
2 aware of, but I believe and will find that the probative  
3 value substantially outweighs the prejudicial effect for the  
4 following reasons:

5 Mr. Maldonado apparently has a continuing pattern  
6 of criminal conduct. If this was a 1991 burglary in and of  
7 itself and nothing else, this Court would be probably in the  
8 position of excluding it. I know I could be criticized  
9 because the easy call is get rid of one prior. Keep two.  
10 Everything is safe. It's not the appropriate call in my  
11 opinion.

12 The similarities are not the same, so the Court  
13 need not be concerned with prejudice.

14 Then the final question for this Court is what is

15 the cascade effect of this in the sense there are so many  
16 priors? Once I have allowed the 2003 attempted exploitation  
17 of a minor and once the Court has allowed the attempted  
18 fraudulent scheme and artifice, whatever prejudice may have  
19 occurred has already occurred because, one, the multitude of  
20 the priors and, two, the type of prior, the exploitation of  
21 a minor. Those are the most dangerous priors in terms of a  
22 light going off in a juror's head and saying I just don't  
23 like this person, let alone I am not going to believe him.

24 But where so much of this case depends on  
25 credibility where you are reaching back to see what the

SHARON SEFFENS, U.S. COURT REPORTER

80

17:52:01 1 character is of a person who is about to take the stand and  
2 make statements that are so pivotal to the case, then this  
3 prior is so substantially relevant that it far outweighs  
4 this Court's belief that there is a prejudicial effect.  
5 Therefore, the addition of that one prior to this Court now  
6 seems minimal having found that the 2003 priors -- both of  
7 them -- are coming before this jury.

8 The Court also notes that I wish we were in the  
9 position of having the United States Attorney's Office  
10 because I would have a CII rap sheet or an NCIC sheet in  
11 front of me, and I could see the whole spectrum of  
12 Mr. Maldonado. I would like to know if Mr. Maldonado has  
13 additional misdemeanors in between, not as a tolling factor.  
14 I would like to see if he has got failures to appear in a  
15 traffic court, but as civil counsel, you can't get your  
16 hands on those unfortunately, so we are all a little blind.

17 I am left with a record of three priors. That's  
18 my only knowledge at the present time. NDS you would have a  
19 much stronger record also if we had a rap sheet and it  
20 showed nothing in between. That's the difference between  
21 civil and criminal law.

22 So Mr. Maldonado will be on the stand tomorrow,

23 and you will be able to impeach him, but I agree with what  
24 NDS said in their papers. Impeachment sounds like this.  
25 Were you convicted in 1991 of a felony prior, a burglary?

SHARON SEFFENS, U.S. COURT REPORTER

♀

81

17:53:44 1 Yes or no? That's the end of it. It is not did you break  
2 into an 84-year-old man's house, et cetera? Did you take  
3 his scrapbook? No. That's the end of it.

4 Were you convicted of attempted exploitation of a  
5 minor in 2003? Yes. That's the end of it.

6 Third -- and the one I worry about the most --  
7 were you convicted in 2003 of an attempted fraudulent scheme  
8 or artifice? Now, the rule says that that's as far as you  
9 can go, but one of you is going to be tempted to stray over  
10 that line.

11 So what are your thoughts? In other words, right  
12 now the rule is you can impeach him, but you can only  
13 impeach him with were you convicted in 2003 of an attempted  
14 fraudulent scheme and artifice felony? Yes or no? But I  
15 don't want NDS then to come back and try to get into that.  
16 That is going to be the rule.

17 So what do you want to do, Mr. Eberhart?

18 MR. EBERHART: We are fine with the Court's ruling  
19 that no additional details be given.

20 THE COURT: Okay. I wanted you to make that  
21 initial call. I just perceived it might be to your  
22 advantage. If it's not, that's the rule, and we abide by  
23 the rules.

24 Okay, thank you very much.

25 (Proceedings were adjourned.)

SHARON SEFFENS, U.S. COURT REPORTER

♀

82

17:55:41 1

-oOo-

2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

SHARON SEFFENS, U.S. COURT REPORTER

♀

83

17:55:41 1

-oOo-

2

3

CERTIFICATE

4

5

I hereby certify that pursuant to Section 753,

6

Title 28, United States Code, the foregoing is a true and

7

correct transcript of the stenographically reported

8

proceedings held in the above-entitled matter and that the

9

transcript page format is in conformance with the

10

regulations of the Judicial Conference of the United States.



11

12 Date: 4/30/08

13

14

Sharon A. Seffens 4/30/08

15

SHARON A. SEFFENS, U.S. COURT REPORTER

16

17

18

19

20

21

22

23

24

25

SHARON SEFFENS, U.S. COURT REPORTER

♀