JAMES A. DiBOISE, State Bar No. 083296
ELIZABETH M. SAUNDERS, State Bar No. 138249
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
650 Page Mill Road
Palo Alto, CA 94304-1050
Telephone: (650) 493-9300
Facsimile: (650) 565-5100

Attorneys for Plaintiffs
GROUPE CANAL+ S.A.,
CANAL+ TECHNOLOGIES, S.A. and
CANAL+ TECHNOLOGIES, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

| | |
|---|---|
| GROUPE CANAL+ S.A., CANAL+ TECHNOLOGIES, S.A., CANAL+ TECHNOLOGIES, INC.,<br><br>Plaintiffs,<br><br>v.<br><br>NDS GROUP PLC, NDS AMERICAS, INC.,<br><br>Defendants. | CASE NO.: C02-01178 VRW<br><br>**DECLARATION OF VINCENT LABIE IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED DISCOVERY AND TO PRESERVE DOCUMENTS AND THINGS**<br><br>Date: April 18, 2002<br>Time: 2:00 p.m.<br>Place: Courtroom 6, 17th Floor |

I, Vincent Labie, declare as follows:

1. I work in the 3SI department of Groupe Canal+ as an electronic and software engineer. My responsibilities at Canal+ include monitoring the development of attacks on Canal+ Technologies's conditional access technology, analyzing counterfeit cards and developing countermeasures to disable these counterfeit cards. I have personal and firsthand knowledge of the matters set forth in this declaration and if called upon to testify regarding these matters, I could and would do so.

2. I have examined counterfeit Canal+ smart cards that appeared in the market after the publication of the UserROM (object code) on the DR7 website in March 1999. The encryption algorithm and the substitution matrixes on each counterfeit Canal+ smart card that I examined are identical to the original encryption algorithm and substitution matrixes that existed and were protected in Canal+'s MediaGuard smart cards prior to the March 1999 publication. The UserROM code of the original smartcard can be used to reconstitute this exact encryption algorithm and substitution matrixes which are required to produce counterfeit cards. The publication of the UserROM code on the Internet in March 1999 enabled the production of counterfeit Canal+ smart cards.

3. The DR7 publication of the UserROM code exposed our encryption algorithm and substitution matrixes to any individual capable of translating the object code back into source code. Many tools exist to automatically perform that conversion and there are many people who can complete this task. After conversion to humanly understandable source code, though it takes time and effort, it is possible without further electrical or mechanical inspection of a card to figure out the keys necessary to decrypt, encrypt and sign messages, which allows descrambling of digital pay television content. The extraordinarily difficult and costly step of extracting the object code from the card was the primary barrier to counterfeiting that version of the MediaGuard smart card.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on April 8, 2002 at Paris, France.

/s/Vincent Labie
Vincent Labie