

1 JAMES A. DiBOISE, State Bar No. 083296
ELIZABETH M. SAUNDERS, State Bar No. 138249
2 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
3 650 Page Mill Road
Palo Alto, CA 94304-1050
4 Telephone: (650) 493-9300
Facsimile: (650) 565-5100

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

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 SAN FRANCISCO DIVISION

12 GROUPE CANAL+ S.A., CANAL+
13 TECHNOLOGIES, S.A., CANAL+
TECHNOLOGIES, INC.,

14 Plaintiffs,

15 v.

16 NDS GROUP PLC, NDS AMERICAS, INC.,

17 Defendants.

) CASE NO.: C02-01178 VRW

)
) **DECLARATION OF VINCENT**
) **LABIE IN SUPPORT OF**
) **PLAINTIFFS' MOTION FOR**
) **EXPEDITED DISCOVERY AND TO**
) **PRESERVE DOCUMENTS AND**
) **THINGS**

) Date: April 18, 2002

) Time: 2:00 p.m.

) Place: Courtroom 6, 17th Floor
)
)
)
)
)

21
22 Je, soussigné Vincent Labie, déclare ce qui suit:

23 1. Je travaille dans le service 3SI au sein du Groupe Canal+ en tant qu'ingénieur en
24 électronique et en informatique. Mes responsabilités à Canal+ incluent la surveillance des
25 attaques portant sur le contrôle d'accès conditionnel de Canal+ Technologies, l'analyse des
26 cartes pirates et le développement de contre-mesures inhibant ces cartes pirates. J'ai une
27
28

1 connaissance personnelle et de première main des domaines abordés dans cette déclaration et
2 dans le cas où je serais appelé à témoigner sur ces sujets, je le ferais.

3
4 2. J'ai examiné les cartes pirates Canal+ qui sont apparues sur le marché après la
5 publication de la UserROM (code objet) sur le site DR7 en mars 1999. L'algorithme
6 cryptographique et les tables de substitutions de toutes les cartes pirates Canal+ que j'ai
7 examinées sont identiques à l'algorithme cryptographique et aux tables de substitutions
8 originaux qui sont présents et étaient protégés dans les cartes à puces Canal+ MediaGuard
9 jusqu'à la publication de mars 1999. Le code UserROM des cartes originales peut être utilisé
10 pour reconstituer cet algorithme cryptographique et les tables de substitutions nécessaires pour
11 créer des cartes pirates. La publication de la UserROM sur Internet en mars 1999 permit la
12 production des cartes à puces pirates Canal+.

13
14
15
16 3. La publication sur DR7 du code UserROM divulgua l'algorithme cryptographique et
17 les tables de substitution à tout individu capable de transcrire le code objet en code source. De
18 nombreux outils existent pour effectuer cette conversion automatiquement et de nombreuses
19 personnes peuvent effectuer cette tâche. Après conversion en code source humainement
20 compréhensible, ce qui nécessite néanmoins du temps et du travail, il est possible d'obtenir, sans
21 plus d'étude physique et électrique sur la carte, les clefs nécessaires pour décrypter, crypter et
22 signer les messages, ce qui permet de décrypter les chaînes numériques de télévision payante.
23 Les étapes extraordinairement difficiles et coûteuses d'extraction du code objet d'une carte
24 étaient les barrières principales à la création des cartes pirates MediaGuard.

1 Je déclare, sous risque de poursuites selon les lois des Etats Unis d'Amérique, que ma présente
2 déclaration est exacte et sincère.

3

4

5

6

7 Sign'e 8 April 2002, à Paris, France.

8

/s/Vincent Labie
Vincent Labie

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28