

## **The Philips' proposal to use a watermark instead of using approved Table A encryption-based content protection technologies cannot effectively protect Marked Content:**

- 1) If encryption is not used to make digital recordings of Marked Content, these in-the-clear digital recordings can be placed into a PC DVD-ROM drive, the content recorded onto the PC's hard drive into its KaZaA sharing folder, and then shared to millions of people over the Internet.
- 2) Reliance on the detection and response to a watermark in lieu of using encryption-based protection would require a change of the regulation from the current:
  - a) detection of and response to the Broadcast Flag in demodulators & modulators that triggers downstream encryption-based protection  
  
to the Philips' proposed
  - b) detection of and response to a Broadcast Watermark by all forms of digital recorders and digital interfaces, in order to trigger redistribution control.

Expansion to such a broad range of devices would significantly increase compliance monitoring and regulation enforcement costs.

- 3) Use of a watermark instead of the much simpler flag increases the costs of marking and the costs of detector implementation. These costs would also include the proprietary watermark licensing costs. This additional cost is unnecessary in this application.

- 4) The use of encryption-based Table A technologies will not be a burden on consumers because next generation DVD players will likely incorporate Table A technology decryption (e.g. 4C CPRM) in their base functionality.
  
- 5) Finally, legacy DVD recorders with analog inputs can continue to make unencrypted copies of Marked Content that will play in legacy DVD players by recording the analog Standard Definition TV outputs of Digital TV receivers.

May 5, 2003