Content Protection
and
Copy Management

Our Concern

- Unrestricted and Unauthorized Redistribution of Digital Broadcast Content on a Worldwide Basis

News Corporation

Source/Sink Device Obligations

- Recognition of Labels Informing of Rights Assertion
- No Alteration of Label Integrity
- Prevention of Retransmission Outside the Home
- Protection of Outputs to Displays

News Corporation

Current 5C License Terms

- Partial Solution
  - Protects Conditional Access Content
- Remaining Problem: Over the Air Broadcast
  - No Protection Against Unauthorized Retransmission
  - No Protection Against Unauthorized High Resolution Format Output

News Corporation

Proposed Solution

- Watermark and Flag Detection in Source Devices to Prevent Retransmission and Unprotected Outputs to Displays
  - ATSC Transport Stream Processing is the application that will cause triggering of protection in DTCP & HDCP
- Consumer Friendly Means of Transitioning From Unprotected to Protected Outputs to Displays

News Corporation

Protection of Display Outputs

- Proliferation of Unprotected High Resolution Display Outputs Will Create a New Class of Unauthorized Digital Recorders (Which Do Not Exist Today) and that Do Not Need 5C.

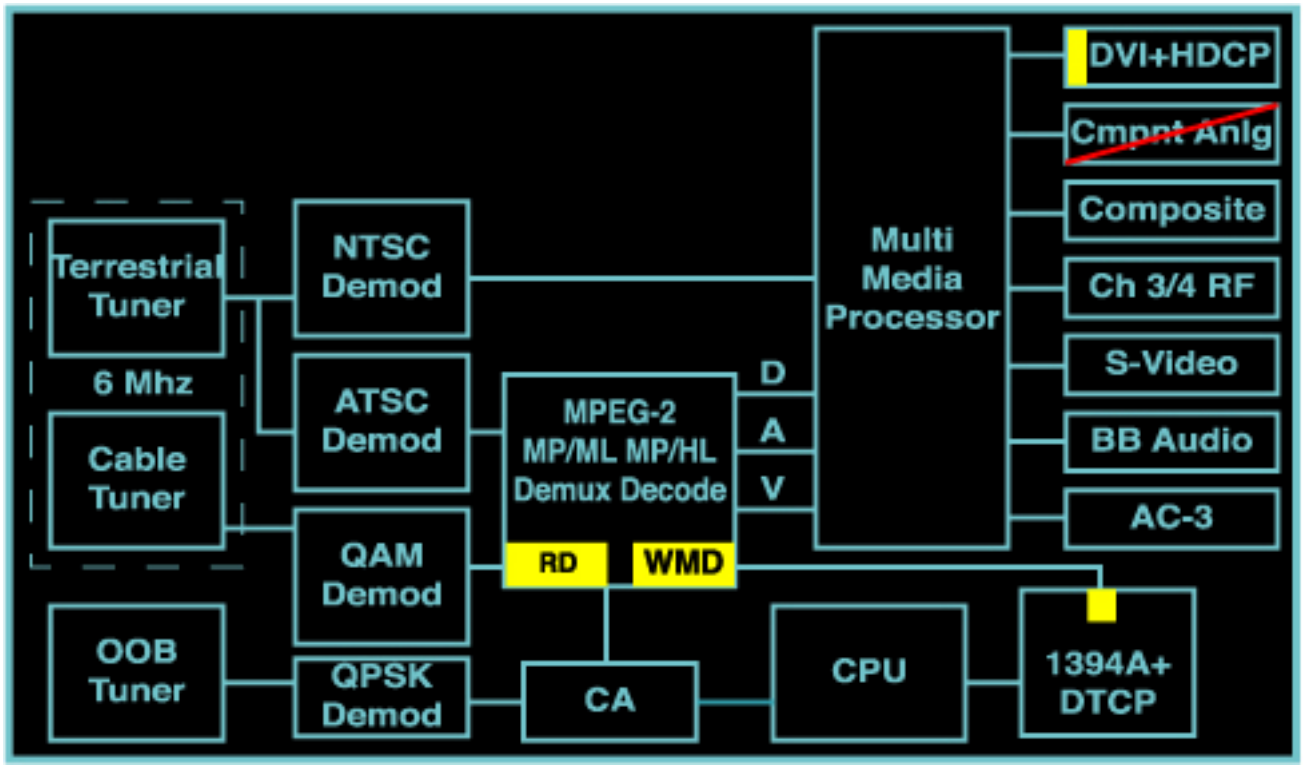
News Corporation

Protection of Display Outputs (contd.)

- All Copyright Owners Agree on the Desirability of Protected Display Outputs
- Encourage Protected Display Outputs Transitioning in a Consumer Friendly Way
  - Continued Availability to Support Legacy Products

News Corporation

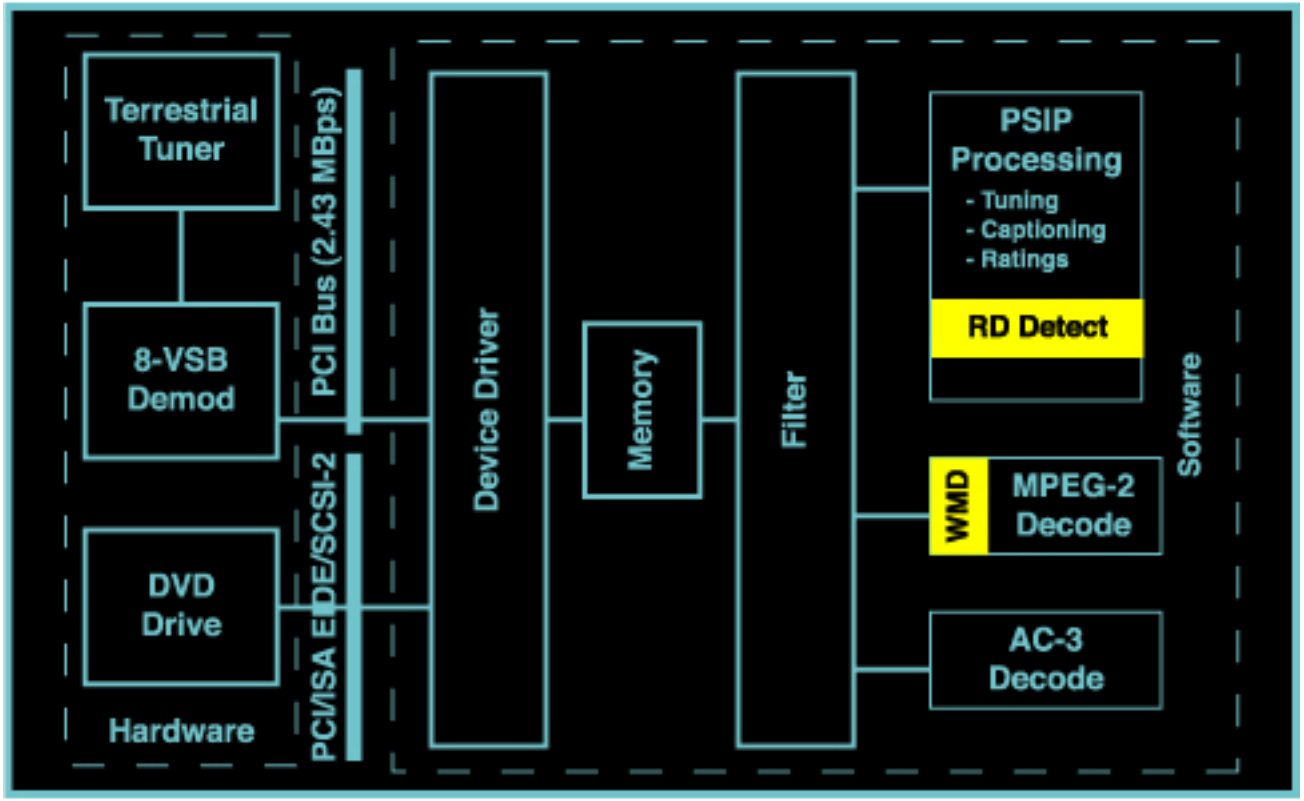
STB/DTV Receiver



RD = ATSC Redistribution Descriptor Detection
WMD = Watermark Detection

News Corporation

PC DVD Player & DTV Receiver



RD = ATSC Redistribution Descriptor
WMD = Watermark Detection

News Corporation

Robustness

ATSC Redistribution Descriptor (RD) processing shall be performed in a secure and robust environment. The environment shall have been designed to effectively foil or prevent circumvention of triggering token identification and subsequent Content Protection and Copy Management (CPCM) processing by knowledgeable persons. If performed within a hardware device such as an embedded processor or specially designed and fabricated silicon, the RD and CPCM processing functionality shall be implemented in such a manner so as to prevent circumvention of signaling to other interconnected hardware devices or software based processes. If performed within a software environment by a general purpose processor whose programming execution is accessible to other processes or devices, the RD and CPCM processing functionality shall be executed at kernel level within a protected memory environment using challenge/response module authentication techniques (using either RSA or DSA algorithms in conjunction with licensing authority assigned signatures) to verify the authenticity of both requesting and receiving driver software processes and using effective tamper resistant software techniques including obfuscation by dynamic segment reshuffling and relocation, encryption, and address translation.