REPORT ITU-R BT.2070

# Broadcasting of content protection signalling for television

(2006)

## 1 Introduction

This Report comprises a report on the current "state of the art" of digital content protection for broadcast television and related services.

Recent rapid evolution in the nature of consumer use of broadcast and internet services has changed many of the old assumptions made by broadcasters and television equipment manufacturers.

Television broadcasts can now be easily recorded using high-capacity personal video recorders (PVRs), and this content can now be shared with others over high-speed internet connections or by burning to high-capacity removable media such as DVDs.

Old assumptions that a set-top-box connects to a single, display-only, television set are fading fast.

Consumers are increasingly aware of alternative ways to enjoy broadcast content, and are always looking for newer and more rewarding experiences.

Accordingly, there is an urgent need for content owners and broadcasters to balance the need to protect their investment with potential loss of acceptability to an educated and technically knowledgeable user community.

### 1.1 Background

Working Party 6M (WP 6M) has determined that a compendium of information should be disseminated and carried forward in preparation for a Report on this subject area.

Building upon the initial work of previous meetings of WP 6M, it was determined that in order to develop principles which can safeguard the interests of broadcasters and the public in copy protection signalling for television, a number of topics need to be addressed.

To this end, WP 6M has begun to develop a content protection model as described below.

ITU-R SG 6 Recommendations for content protection need to address the requirements identified for each of the reference points and subject areas identified in the model.

The administrations attending WP 6M concurred that this new area of applying security to broadcast material presents challenging topics, and thus great care and deliberation must be taken in creating Recommendations. Further information in accordance with the work programme will be gathered.

### 1.2 Sources

This Report was prepared based on a number of past input documents provided to ITU-R WP 6M, and on public documents and materials suggested to the Rapporteur.

### 1.3 Working method

At the April 2005 meeting of WP 6M, it was agreed that the total aggregate volume of contributions on this subject was too much for a simple report. The Rapporteur was therefore requested to produce a "digest" report summarizing the issues and solutions described in the various submissions.

As such, this Report is now intended to summarize what WP 6M has learned so far in this process. Many of the submissions are mentioned explicitly in the text below, while others have been considered without an explicit reference.

The Rapporteur now anticipates a period of consideration for future direction, along with comments made against previous and current text in this Report. This remains a "living document" which will evolve over time, and nothing contained herein constitutes finalized or formally agreed text.

## 2 The threats to the industry

This section describes some of the commercial threats to broadcasters and content providers resulting from advances in technology. However this list is not exhaustive.

### 2.1 Commercial piracy

Commercial reproduction of broadcast material includes the mass production of DVD versions of movies and television series, and the sale of content through unlicensed internet services.

It may also include the sale of technology (or advertising therein) that is clearly intended to promote piracy although the software vendor does not directly profit from the act of piracy.

### 2.2 Casual piracy

This includes consumers who make single copies of movies and other content as gifts for friends or family members with no intent for personal gain. Recent research indicates that most consumers feel this is normal and inevitable activity, though it remains a potential violation of copyright law.

### 2.3 Region leakage

For some content, broadcasters negotiate the right to transmit based on geographical coverage. These agreements typically allow for a certain amount of leakage, e.g. across terrestrial broadcast boundaries. However, excess leakage for other broadcasters (via internet, satellite footprint or otherwise) can reduce the value of that content for other broadcasters.

NOTE 1 – This effect is unrelated to DVD region coding, and is perhaps most noticeable for content with a very short commercial lifetime such as sporting coverage.

### 2.4 Early window viewing

Often related to region leakage, this involves audiences having access to content while it is meant to be restricted to another format. For example, being able to obtain DVDs while a movie is still in local theatres, or seeing content from a foreign free-to-air broadcast while it is only available on pay-per-view in the local market.

The effect of early opportunities for viewing is to reduce the revenue potential for existing legitimate licensees of the content, as the potential market shrinks.

### 2.5 Loss of advertising revenue

Services that depend on advertising for some or all of their revenue are vulnerable to loss of revenue from any of the above effects, or as a result of advertisement-skipping. However, most consumers feel strongly that they have a right to avoid adverts they find annoying, whether for products they don't want or need, or for products they find distasteful to think about. As always, a balance needs to be struck.

### 2.6 Derivative works

With today's ease of capturing and editing material, there is a growing risk of copyright works being reused and adapted without permission. For example reusing a soundtrack for another purpose, or developing an unofficial re-edited version of a movie beyond the bounds of permitted fair use.

### 2.7 Poor implementations

Where content protection is mandated, there is a threat to compliant device manufacturers from competing products that do not meet the same standards of protection.

The usual "market will choose best implementations" actually runs in reverse for content protection, where often the (informed) consumer will choose the *least secure* implementation if it provides a perceived greater ease of use or flexibility.

As evidence of this in other markets, readers should consider the relative attractiveness of DVD players that ignore the DVD region code (which are now commonly available in many countries), or cell-phones that are "unlocked" from their original (subsidizing) service provider. Indeed, DVD region coding has recently been declared anti-competitive, and therefore illegal, by the European Commission.

## 3 The challenges for legitimate use

Balancing the fears of content providers arising from the threats noted above, there are a number of corresponding fears over excessive corporate control of consumer use of broadcast television services.

Throughout the industry there is considerable debate over the technical sensibility of providing both adequate protection and flexibility of use to consumers for the same item of content.

### 3.1 Legitimate fair use

In many countries, there are historical principals of fair use that are recognized in legislation or common law. These vary greatly between jurisdictions, so there are no hard-and-fast rules for what should be allowed.

Some of these are not well solved through use of technology (such as expiry of copyright material into the public domain), but blocking certain other rights may result in consumer complaints, regulatory restrictions, or legal challenges to content protection technologies.

The digital media project (http://www.chiariglione.org/project/) has attempted to identify a number of "traditional" rights consumers associate with content they "own" in today's world of television and digital media. How applicable these traditional rights are in the world of rapidly evolving technology is a subject of intense debate.

### 3.2 Accessibility

Of specific interest are the traditional rights employed by those working to assist people with various disabilities, for example the RNIB (http://www.rnib.org.uk) and RNID (http://www.rnid.org.uk/) who are very active in UK policy making.

#### 3.2.1 Application usability

As television becomes increasingly interactive, there is a risk that some of the audience will be denied access to content due to inability to use some of the interactive applications that make it available. For example, content protection mechanisms that complicate the user interface may become awkward for users with limited vision.

#### 3.2.2 Addition of subtitling and descriptive audio

Examples include volunteers adding descriptive audio to television shows for the visually impaired, or overlaying signing for the hard of hearing. The modified shows would then be made available to the relevant community.

Both of these examples can be hampered by content protection technology, leaving those groups entirely dependent on the timely delivery of these features by the original content producers.

This is further complicated for those who rely on subtitling for less common languages.

### 3.3 Education and academia

It is a traditional right of academia to employ extracts of copyright works of many kinds for use in academic study, criticism, or as teaching materials. Content protection technology can make this onerous or impossible.

### 3.4 Public service obligations

Some broadcasters are bound by public service obligations such that content they transmit must be made available to all legitimate users without any technical barrier. In such cases it is often unlawful to require any form of subscription to the service – the user is already recognized as a subscriber because they live in the territory and pay the relevant license or tax, so they already have right of access to this content which cannot be denied by the broadcaster.

### 3.5 Open source software

Content protection technology often depends on some form of trust model, with some degree of robustness in the device before it is trusted with valuable content (see § 5.2.2). However, those companies and individuals adhering to the strict principles of open source software may be unable to prove robustness, as their software can be changed by anyone using the provided source. There is therefore a fear that this community will be forever denied access to broadcast television content despite the innovations they might be able to contribute to the industry.

Others will contend that open source software is inherently insecure and as such is an inherently unacceptable development methodology for systems that must protect content.

Both camps have some strong proponents.

### 3.6 Public domain material

In some territories there is fear that content which is already in the public domain could become over-controlled by making it available under broadcast content protection, thus denying by technological means the legitimate rights that users have with public domain material. Some broadcasters fear legal exposure if accused of this.

### 3.7 Creative commons

A recent innovation in the publication of content is the use of creative commons licenses. These allow for the non-commercial creative reuse of the labelled content, provided that the original author is credited. This approach is attractive for smaller content providers such as independent artists and authors, as it allows their work to flow and become far more visible. A variant of creative commons allows for commercial use by residents of developing nations. Some major broadcast organizations are now adopting creative commons as a means to give consumers and other content creators access to their archival materials in a useful manner.

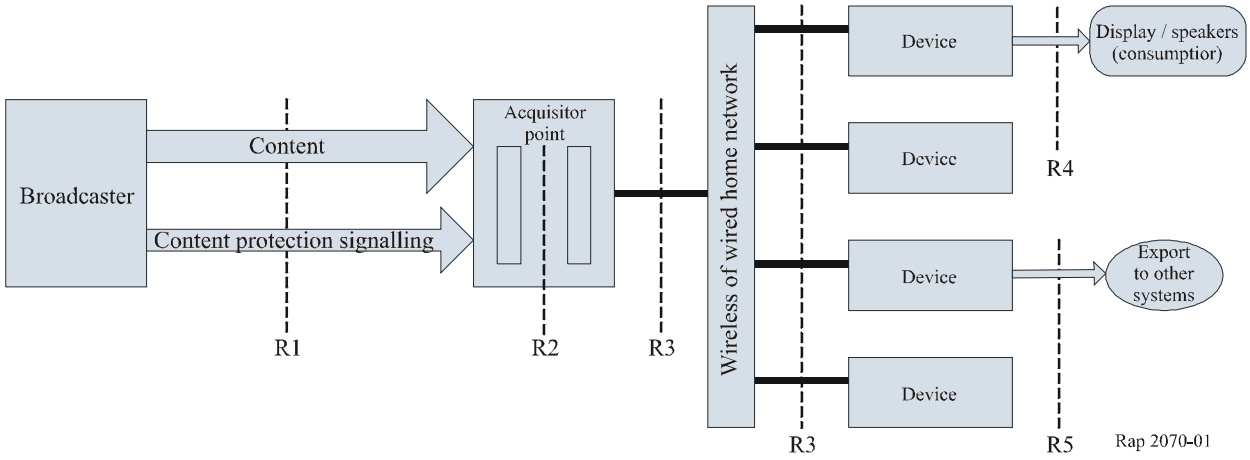
## 4 Architectural model

Content protection for broadcasting is a very complex subject, and many well-known proposals solve only part of the bigger puzzle.

ITU-R WP 6M will therefore use the following model to identify areas of study.

FIGURE 1

**6M content protection model**

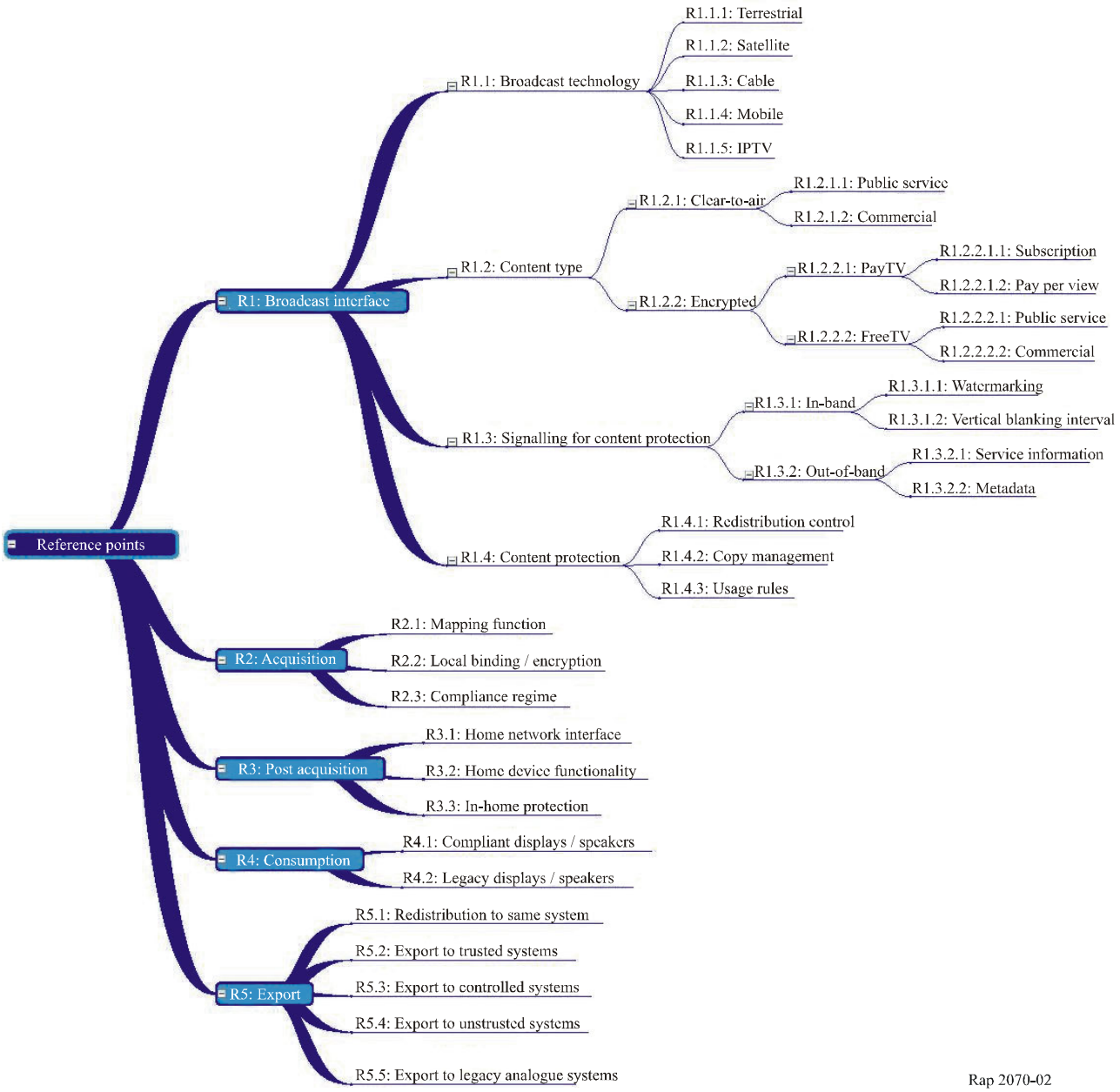



With this diagram we define a set of reference points at which requirements and/or solutions need to be defined. Some of the terminology used is based on the DVB (http://www.dvb.org) CPCM concepts.

The following diagram further breaks down these reference points into topics for consideration or study.

FIGURE 1

**Expanded reference points**




## R1: Broadcast interface

R1 lies between the broadcaster and the first receiving equipment in the home. The following subject areas apply at R1:

### R1.1: Broadcast technology

Content protection mechanisms are required for different broadcast technologies. While each is somewhat different, there are clear benefits to harmonization across these platforms.

**R1.1.1: Terrestrial**

For example DVB-Terrestrial and ATSC broadcasts. Analog broadcasts may also be considered.

**R1.1.2: Satellite**

For example DVB-S and DVB-S2, and equivalent systems.

**R1.1.3: Cable redistribution**

Delivery over cable systems, while out of scope for ITU-R, is relevant for reasons of interoperability and ease of deployment, both for broadcasters and for consumers.

**R.1.1.4: Mobile**

Delivery over specialized radio networks for mobile and/or handheld devices. Examples include the DVB-H variant of DVB's terrestrial broadcast system. Some of these systems use an IP protocol layer to carry content.

**R.1.1.5: IPTV**

Television delivered over a broadband IP-based network such as DSL, wireless DSL, or cable modem. This is mostly out of scope for ITU-R, but should be considered for interoperability reasons.

**R1.2: Content**

The content delivery system may carry content of various kinds. This can affect the type of protection (if any) to be applied.

**R1.2.1: Clear-to-air**

Content is not scrambled for security. This does not preclude scrambling for pure transmission reasons. Such content can be used in-the-clear without requiring keys or control words.

Clear-to-air includes public broadcast services that are funded in whole or in part by government mechanisms, and/or which have public service obligations, e.g. universal access, together with services that are funded in whole or in part through the sale of advertising. Some services operate as a combination of these two.

**R1.2.2: Encrypted**

Content is scrambled (encrypted) prior to transmission. Receivers need to have access to control words or keys before they can descramble and access the clear content.

**R1.2.2.1: PayTV**

Traditional PayTV services where receivers include additional technology to decrypt the content to which they are entitled. These are typically protected by conditional access systems.

**R1.2.2.1.1: Subscription**

Subscription services usually operate by enabling access to channels based on the package being paid for on a regular basis. Protection is applied to the whole channel and access is granted continuously.

**R1.2.2.1.2: Pay-per-view**

Reception of pay-per-view content is for a given content item, usually on a specific channel at a given time.

#### R1.2.2.2: Free TV

In some territories, free television services are scrambled in some way (e.g. conditional access) for reasons other than the enforcement of payment for the service, e.g. to mitigate cross-border leakage into neighbouring countries.

##### R1.2.2.2.1: Public service

See under R1.2.1.1. Some public service broadcasters have chosen to employ encryption on their broadcasts for a number of reasons, for example to prevent region leakage. In other cases, this is done because it is a requirement of the network (e.g. a satellite operator) rather than of the broadcaster.

##### R1.2.2.2.2: Commercial (advertisement-supported)

See under R1.2.1.1. Generally, the reasons outlined in R1.2.2.2.1 also apply here.

### R1.3: Signalling for content protection

Signalling for content protection is the transmission of control information and/or commands to receivers of protected content.

#### R1.3.1: In-band

In-band signalling is carried within the primary media stream. As such it will normally be carried throughout the entire chain to the final display, unless deliberately removed.

##### R1.3.1.1: Watermarking

Watermarking refers to the inclusion of hidden information directly in the video or audio stream of the content. Ideally this will be invisible/inaudible to the human viewer, but will successfully survive media conversion to other formats.

##### R1.3.1.2: Vertical blanking interval

An area of non-visual information located between the frames of an analog television video signal, often used to carry Teletext, closed captions, and other service information.

#### R1.3.2: Out-of-band

Out-of-band signalling is carried independently of the primary media stream. This signalling will often be lost at reception. As such, it will usually need to be mapped to another system once the content is acquired by the user.

##### R1.3.2.1: Service information (SI)

Data carried in the MPEG2 transport stream. This information is typically lost at acquisition.

##### R1.3.2.2: Metadata

Rights information may also be sent as additional program metadata, for example in an enhanced electronic program guide which may be transferred separately from the content itself.

### R1.4: Content protection

The type of protection to be applied to the content may come in several forms.

#### R1.4.1: Redistribution control

The simplest form is a simple redistribution control signal, indicating that content cannot be sent beyond a defined space.

The USA's broadcast flag regulation is one such example. However, this approach also has a long history in the mobile arena where a forward lock flag is used to prevent sharing of ring-tones and similar mobile phone content items.

**R1.4.2: Copy management**

Copy management allows the content owner to control the way copies are made of the content, whether logical on disk or physically to optical media. The most common form of this is with so-called CCI bits, usually standing for:

– Copy never
– Copy once
– Copy no more
– Copy control not asserted.

**R1.4.3: Usage rules**

More sophisticated systems allow the content owner to confer more complex rights on the user. This requires a richer signalling system, either a more complex flag structure or a full rights expression language (REL).

**R2: Acquisition**

Acquisition is the process of the user receiving the broadcast content and putting it under local protection in the device(s) in the home. In many cases this will involve the removal of the protection applied during broadcast, and the application of a new protection means.

**R2.1: Mapping function**

Mapping consists of taking the usage information from the broadcast signalling, and converting it to a form that the in-home system can use. This is done using mapping rules defined by some form of compliance regime. There may also be local legal requirements on specific mapping cases.

**R2.2: Local encryption/keys**

With the rights converted, the content often has to be re-protected. This may involve re-encryption of the content itself using a key specific to this user or group of devices.

**R2.3: Compliance regime**

A compliance regime is required to determine what the mapping rules are, and to define the compliance and robustness requirements for devices that will be allowed to use this. The regime is required to prevent the development of legal but non-conformant alternative devices that do not provide satisfactory protection.

**R3: Post-acquisition**

This reference point identifies the device-to-device interactions between television devices owned by a single consumer or household. This interface is used to share the content that the consumer already has rights to use.

**R3.1: Home network interface**

An example of this could be a home Ethernet or wireless network, perhaps using protocols developed by the DLNA. Other examples could include IEEE 1394 Firewire, USB 2.0, or direct cable connections such as DVI or HDMI.

**R3.2: Home device functionality**

Television and radio-related functions that may be present in devices within a modern home include:

– Acquisition of content (e.g. tuner or equivalent)
– Storage (e.g. on hard drive, or on removable media such as DVD burning)
– Processing (e.g. transcoding, permitted editing)
– Consumption (e.g. screen of speakers for presenting content to humans)
– Export (e.g. passing to another protection system, legacy systems, or the internet).

Any given device type may include any combination of these functions, and perhaps others that are not broadcast related such as games. Manufacturers will continue to implement consumer devices in innovative ways, and the content protection arrangements must be flexible enough to operate in such an environment.

However, for some device classes, content is protected inherently by the nature of the device. For example, a pure television set (consumption function only) having no electric outputs for content, cannot be used to make digital copies by its very nature.

**R3.3: In-home protection**

Content flowing between devices in the home needs to be sufficiently protected. This will usually mean the use of either content or link protection. These are discussed in section 5.3 below.

**R4: Consumption**

Consumption is the presentation of broadcast content to human users, as light and sound.

**R4.1: Compliant displays/speakers**

This refers to displays known to meet the requirements of protecting the content, being equipped with suitable protocol stacks and meeting the relevant compliance/robustness rules.

**R4.2: Legacy displays/speakers**

In addition to compliant displays, there will be for many years a large installed base of legacy equipment, both analog and digital, which still has to be supported. To ensure these signals are only used for human consumption of content and not for recording remains a known problem.

**R5: Export and redistribution**

Most content protection systems have concepts of export and redistribution. Export usually refers to content moving from one *technology* to another, while redistribution usually refers to content flowing to another *user* of the same technology.

**R5.1: Redistribution**

This reference point refers to content leaving the current household to another, perhaps a neighbour or friend.

**R5.2: Export to trusted systems**

This reference point refers to content flowing from one protection system (A) to another (B) which is fully trusted by the compliance regime of first. The second system assumes all control of the content. A mapping between the two systems will have been developed by the relevant compliance body(s), and all implementations of devices using both systems will follow this. Trusted systems are permanently enabled.

**R5.3: Export to controlled systems**

Similar to R5.2, however in this case the second system is not always trusted, and the export to a specific controlled system may be controlled (switched on or off) on a content-by-content basis.

**R5.4: Export to untrusted systems**

Also similar to R5.2, but in this case the output system is known to be untrustworthy (e.g. unprotected DVI), and the export to the untrusted set of systems is controlled (switched on or off) on a content-by-content basis.

**R5.5: Export to legacy analog systems**

Analog television systems remain a special part of reality of in-home networking. This reference point covers

## 5 Concepts of content protection

This section attempts to explain some of the more common concepts and techniques that could be included in solutions.

### 5.1 Protection during distribution

The following techniques are commonly applied to protect television content during broadcast distribution.

#### 5.1.1 Conditional access

Conditional Access systems are primarily intended to protect from theft of the *service* rather a specific content item. This is achieved by encryption of the broadcast content (often referred to as "scrambling") with a single, frequently changing key (control word). In the European CA architecture defined by DVB, the control words are also transmitted to the receiver inside encrypted messages (known as ECMs and EMMs) that are only accessible by specific receivers (or groups of receivers). The logic to decrypt these messages is often held in a secure smart card. Once the content is descrambled, the CA system takes no further part in protection, though the CA vendor may impose requirements on acquisition equipment and interfaces.

#### 5.1.2 Digital rights management (DRM)

Digital rights management is an integrated approach to content protection involving the protection of data with encryption, and the delivery of keys to unlock this data provided that the recipient meets certain conditions defined by the sender in a "rights expression language". DRM assumes the presence of a suitable DRM client that is trusted to evaluate rights, decrypt content, and grant access to the unencrypted data when appropriate.

In a DRM system such as "OMA DRM" or the various proprietary technologies such as "Windows Media DRM", content may already be encrypted and wrapped in a DRM file format prior to broadcast. This format would usually be retained through to the end device.

#### 5.1.3 Clear-to-air signalling

For unencrypted broadcasts, content protection signalling may be included in-band or out-of-band. There is an inherent insecurity in this approach, as there is no technical barrier to consumers implementing a receiver that ignores this signalling while extracting the content. However, this risk can be mitigated through use of a regulatory framework such as that proposed for the US broadcast flag regulations (see § 5.2.1.1), which would prohibit the use of receiver that do not adequately implement the behaviour required by the signalling.

### 5.1.4 Watermarking

In addition to the technologies mentioned above, there have also been proposals to use watermarks embedded in transmissions to indicate the presence of protected content. The watermark is a digital code hidden in the picture and/or audio of the content, which in theory is difficult both to locate and to remove. This can be used in two main ways; firstly for forensic purposes to determine the source of stolen content, secondly as a way to trigger protection in equipment that recognizes the watermark. The former use is generally accepted, but the latter raises considerable controversy, particularly among equipment makers who fear liability lawsuits from both content owners and consumers should the technology fail to work exactly as intended.

## 5.2 Protection at acquisition

When content is received in a broadcast tuner or equivalent, the protection applied on the broadcast is removed and the content is either stored or passed to another device within the home.

Once content is within the home, some means are required to prevent it being abused.

### 5.2.1 Regulation of receivers

Regulations can be used as one means to enforce correct behaviour by television equipment in the home. Typically this will require both elements of mandation (to require equipment to implement a solution) and anti-circumvention (to prevent users modifying compliant equipment to suppress the protection).

#### 5.2.1.1 "Broadcast flag"[1]

As described in past US contributions to ITU-R WP 6, the US broadcast flag concept defines both an over-the-air signalling mechanism, and a regime of compliance. This operates by requiring all television devices to implement one or more approved technologies (from a set known as "Table A") to keep flagged content secure.

While the original broadcast flag order of the FCC was overturned in court on jurisdictional grounds, there are currently new moves in the US Congress to provide a legislative basis for such a regulation.

### 5.2.2 Commercial compliance regimes

A compliance regime defines the rules under which a device is permitted to access protected content.

Such a regime will typically include the following elements:

– Technical compliance tests, to ensure devices from different manufacturers are interoperable with one another.

– Root of trust, a trusted authority so that devices are able to verify one another's trustworthiness under the regime.

– Robustness rules, to ensure devices are built to an adequate level of security, for example to ban devices that expose unprotected content on open wiring.

– Mapping to/from other systems, to determine correct behaviour when content is received from or delivered to another content protection system.

---

[1] The legal status of the US broadcast flag regulation is being re-evaluated at this time, and readers are advised to check with other sources.

Some regimes may allow self-certification of compliance by manufacturers; others may require third-party (or even governmental) evaluation; and still others will rely on a mix of the two approaches.

For any given standard, a compliance regime may be managed as part of the body that establishes the corresponding technical standard, or it may be managed by a free-standing body that provides the regime as a service to implementers of the standard.

#### 5.2.2.1 Commercial/proprietary

For vertical markets such as pay-per-view, television network operators typically apply their own compliance regimes on purely commercial grounds. For example, a pay-TV satellite operator will contract with a set-top-box manufacturer to include both a conditional access system (to unscramble the broadcast) and one or more protection technologies on connections going to other devices in the home.

The same approach is adopted by companies offering proprietary content protection technologies, as Microsoft does for Windows Media DRM.

#### 5.2.2.2 Content management license authority (CMLA)

The CMLA (http://www.cm-la.com/) provides a free-standing compliance regime for implementations of "OMA DRM 2.0", using "Hook IP" (see below) to provide a legal framework.

However, note that CMLA does not cover all possible uses of "OMA DRM". In particular, CMLA assumes unicast delivery of content to a single receiver, and the trust model does not currently support broadcast distribution.

#### 5.2.2.3 DVB-CPCM compliance

The DVB project (http://www.dvb.org) is providing the specification for the CPCM content protection system. However it is unlikely that DVB itself will provide a compliance regime, and it is anticipated that there may be more than one regime established for different business models (e.g. PayTV and free-to-air).

#### 5.2.2.4 "Hook IP"

"Hook IP" is a special patented invention that is necessary to build a compliant implementation of a standard. The Hook IP must be licensed, and a condition of this license is that the implementation must obey the terms of the corresponding regime. This provides a legal structure to enforce correct implementation independent of any regulation.

### 5.2.3 Anti-circumvention laws

Even with a compliant implementation, there is the threat of circumvention, where a deliberate effort is made to break the protection mechanism in a non-compliant manner. As noted above, products that include such circumvention may have unfair market attractiveness.

Anti-circumvention law provides a legal deterrent to this type of activity.

The United States "Digital Millennium Copyright Act" (DMCA) provides a generic framework to counter circumvention of content protection. Similar legislation has been passed, or is under consideration, in other territories.

Legislation of this kind is often seen as threatening to consumer and competitive rights as noted in section 3 above, and can raise considerable controversy.

### 5.3 Protection after acquisition by the consumer

Compliant receiver devices need to protect television content as they hand it off to other devices in the home (or beyond).

#### 5.3.1 Signal disruption

In analog television, a number of proprietary technologies can be applied to the outgoing signal to allow viewing of content while preventing recording, such as Macrovision and Dwight-Cavendish. Modern VCRs and DVD recorders are designed to recognize these disruptions even though it would be technically possible to ignore them.

While this Report is concerned primarily with *digital* television, there is a huge legacy of *analog* television displays and other equipment still present in the world, and any solution must allow for the continued use of such displays for many years to come.

#### 5.3.2 Simple signalling

Some systems rely on setting simple bits in the transmission structure. This also requires a compliance regime to maintain protection.

#### 5.3.3 Watermark analysis

It has several times been proposed that watermarks could be used to protect content in the home. However this raises technical and legal issues for device manufacturers, and many are sceptical that an effective watermark can be designed which can be reliably detected, and yet difficult to remove.

#### 5.3.4 Link protection

Link protection mechanisms work by encrypting content on an individual connection, often using a temporary key used for a single session.

Examples of link protection include HDCP and DTCP-IP.

In each case, the security of an end-to-end chain of devices relies on the set of protected links, and the compliance of each device in the chain.

These links are often formed dynamically as required, based on proximity of the devices being linked. This approach has the advantage of allowing dynamic associations between devices, however it has limitations in establishing trust with devices that are in remote locations.

#### 5.3.5 Conditional access (CA)

Some solutions are based on extending the conditional access paradigm beyond the initial tuner and all the way to the final display device. Examples of this approach include SmartRight and SVP. This approach has the advantage that it supports some innovative business models such as pre-loading of content prior to purchase. However it requires additional complexity in every display device, it prevents devices from extracting clear content (e.g. stills or audio levels) other than for pure display, and it often cannot cope with a consumer combining services from multiple service providers.

#### 5.3.6 Digital rights management (DRM)

DRM systems vary, but they are all based on the concept of encrypting some or all of the content using device- or user-specific keys, and allowing access to those keys only to compliant implementations that will obey the rights granted.

#### 5.3.6.1 Proprietary DRM

There are a number of proprietary DRM systems available across the world, of which the best known are probably "Windows Media DRM" from Microsoft, "FairPlay" from Apple (used for the iTunes service and the iPod music player, and "Helix" from Real Media.

Collectively, these systems provide the vast majority of content protection for media on today's internet and in-home networks.

#### 5.3.6.2 Standardized DRM

While proprietary DRM still dominates the marketplace, efforts are being made to provide a standardized solution.

##### 5.3.6.2.1 OMA DRM

The Open Mobile Alliance has standardized a DRM solution known as "OMA DRM", which is now in version 2.0. This was originally targeted at cellular phone applications, but is now being considered as a broader solution.

### 5.3.7 DVB-CPCM

The DVB (http://www.dvb.org) approach to content protection is rather different to any of the others described above.

Firstly, there is no controlled service provider. Content can be obtained from multiple providers and used across the authorized domain of devices.

Secondly, the current architecture does not always require encryption of the content. In fact, current proposals include a usage state information (USI, the CPCM mechanism for expressing rights) flag to indicate that content should *not* be encrypted by CPCM.

In this sense, CPCM acts like either a link protection system or a DRM system depending on the USI for an individual content item.

## 5.4 Approaches to interoperability

Possibly the only requirement of content protection that is shared by all parties is the need to provide maximum interoperability between solutions, such that consumers are able to move content legitimately between their devices without having to buy them all from a single source.

There are a number of approaches to this goal and there is much less consensus on which to pursue.

### 5.4.1 Single standard

There is a philosophical argument over whether standardized protection can provide the same level of protection as a proprietary approach. There are clear market reasons to allow competitive implementations of a single standard, however there are concerns in some quarters that a standardized approach is inherently less secure.

Part of this arises from the need to make all algorithms completely public, though of course secrecy is not a total solution to the prevention of reverse-engineering.

However there is a bigger concern that a standardized DRM approach is relatively unable to respond to a successful attack, and that no one company can be called to account or ensure that a "fix" is rolled out in a timely manner.

By contrast, a market place solution, relying on multiple vendors, provides incentives to develop effective measures to content protection.

### 5.4.2 Flexible standard

MPEG IPMP proposes a standardized framework that allows for negotiation of content protection mechanisms between devices, such that devices exchanging content agree on a combination of tools they can both support.

### 5.4.3 Bi-partisan agreements/approved outputs

Different content protection technology owners may agree to support one another on their technologies. For example, a link protection standardization group may approve one or more proprietary DRM systems as acceptable alternative outputs. This allows a device manufacturer to build a box that implements both systems and legitimately hand off content between them.

Both bodies would then collectively agree on appropriate mappings of the rights information between the two signalling systems.

In some cases, there may be no way to exactly map between some combinations of expressed rights. This can greatly complicate the negotiation process.

As such, this is a partly technical, but often mostly legal/commercial, process.

### 5.4.4 Multilateral agreements

Going beyond bilateral agreements, it may also be possible to establish "pools" of multilateral agreement, where the whole pool agrees a minimum feature set and then all agree to treat other members as acceptable outputs.

The same issues arise as in bi-partisan agreements, but with more seats at the table.

The coral consortium (see below) is just one example of such an effort.

#### 5.4.4.1 Coral

The coral consortium (http://www.coral-interop.org/) is a cross-industry group seeking to promote interoperability between digital rights management (DRM) technologies used in the consumer media market. Unlike OMA, Coral is not attempting to define a standardized DRM, but has already released a specification for an implementation that would permit different DRMs (both proprietary and standardized) to interoperate with one another. Coral's stated goal is to create a common technology framework for content, device, and service providers, regardless of the DRM technologies in use.

### 5.4.5 Selectable output control (SOC)

Selectable output control is a controversial mechanism whereby the rights granted to a given item of content also identify which technologies it is permissible to hand the content to.

#### 5.4.5.1 Arguments for SOC

SOC advocates argue that as new business models emerge with higher-value content (e.g. movies still showing in theatres), they need to be able to ensure that only the most trusted interfaces are allowed access to it, and that they should be able to disallow content flowing to technologies known to have been breached.

#### 5.4.5.2 Arguments against SOC

The opponents of SOC complain that there is no way for a device manufacturer or consumer to know in advance which technologies are going to be supported in future content releases, so they have to either "guess a winner" or supply/purchase additional sockets/connectors and cables for many different technologies just to avoid the risk of getting a dark screen. Each of these technologies has a cost associated with it, both in materials and in licensing fees, so manufacturers feel that SOC would add an unacceptable level of risk in designing devices, as well as greatly confusing consumers who want it to "just work" reliably.

## 6 Relevant organizations and technologies

The following organizations have provided input texts to ITU-R WP 6M, or to the Rapporteur, or are known to be actively involved in related activities.

### 6.1 MPEG

Moving picture experts group (http://www.mpeg.org)

### 6.2 DVB

Digital video broadcasting project (http://www.dvb.org).

### 6.3 OMA

Open mobile alliance (http://www.openmobilealliance.org/)

### 6.4 EBU

European Broadcasting Union (http://www.ebu.ch)

### 6.5 ATSC

Advanced television systems committee, Inc. (http://www.atsc.org/)

### 6.6 Digital media project

Digital media project (http://www.chiariglione.org/project/)

### 6.7 Coral consortium

Coral consortium (http://www.coral-interop.org/)

### 6.8 EFF

Electronic frontier foundation (http://www.eff.org)

### 6.9 ARIB

Association of Radio Industries and Businesses (http://www.arib.or.jp/english/)