Flag Waving in the Digital Jungle

David Brennan*

A broadcast flag is an electronic notice which is associated with a digital broadcast. Flags are not effective technological protection measures in the sense understood in copyright. As merely a piece of descriptive code embedded within a broadcast, flags do not *per se* lock, encrypt or scramble broadcasts prior to reception. Instead the code is merely a request that hardware receivers limit what can be done with the broadcast after reception. Regulatory mandate of hardware compliance with a flag request is the consequence of this light-handed nature. This chapter will: attempt to describe and explain flag technologies formulated in the US and Europe; contrast the quite unique Japanese solution which encrypts at the source of broadcast; consider the extent to which current Australian regulatory settings cater for flags; review the relevance of the draft WIPO Broadcasters' Treaty to flag technologies, and conclude by suggesting a legal framework for flags as a special type of electronic rights management information.

Introduction

This chapter will attempt to describe and explain an emergent feature of digital broadcast standards, which in the US is known as the 'broadcast flag' and in Europe as the 'content protection and copy management' (CPCM) system. In this chapter they will each be referred to as flag technologies, for while they differ as to detail, they share the same fundamental nature. While more has been published on the US broadcast flag, the European CPCM flag is more recent and sophisticated, and is being formulated within the same digital broadcasting standard applicable in Australia. The chapter will also contrast the quite unique Japanese solution which encrypts at the source of broadcast.

It is convenient by way of introduction to attempt to more generally situate broadcast flag technologies and regulations. Terrestrial broadcast television is often referred to as free-to-air because it is typically distributed freely without technical restriction or limitation ('in the clear') to all who fall within its geographic footprint. Those within that broadcast footprint can freely receive the signal through generally available reception equipment. This free-to-air quality generally arises from the public nature of the allocation and licensing of the broadcast spectrum. Public policy has traditionally ensured that the spectrum so allocated will only be used on a free-to-air basis.

---

* B Comm LLB(Hons) PhD GCertUniTeach (Melb). Senior Lecturer, University of Melbourne Law School and Copyright Consultant, Screenrights – the Audio-Visual Copyright Society. This chapter is based upon a conference presentation entitled 'Waving the Flag in the Digital Jungle' given at the 12th Annual ACIPA Copyright Conference: From The Da Vinci Code to YouTube, Brisbane, 16 February 2007. I would like to thank John Orlando of CBS and Ted Shapiro of the MPAA for sharing their experience with me. Responsibility for the analysis, however, rests entirely with me: d.brennan@unimelb.edu.au

Since at least the audio compact disc in the mid-1980s, digital delivery for the supply of mass entertainment has proliferated. From the mid-1990s the Internet has emerged as a new means to deliver digital content to a mass market without the need to manufacture individual copies. In an Internet-connected world, a single digital copy made available on the Internet is subject to uncontrollable copying and further distribution – leaving to one side bandwidth and congestion issues. Members of the Internet-connected public have at their disposal the means to access and publish material like never before. Therefore, in reaction to the possibility of unauthorised and uncontrollable Internet distribution destroying markets for the sale of such content, copyright owners have, and copyright law has, responded by resort to technological protection. Part of the Internet 'copyright answer' has been the use of, and the giving of legal protection to, digital rights management (DRM) technologies. Through such measures business strategies are emerging to convert unauthorised Internet distribution into authorised market avenues.

At the same time in developed economies terrestrial broadcasting is in the process of converting to exclusively digital delivery, a process likely to be completed within the next five years. For an audio-visual producer (and copyright owner) who wishes to digitally distribute its titles in an Internet-connected world it is faced with a plurality of choice. This choice has been described by the Motion Picture Association of America (MPAA) in a 2005 paper in these terms:

> Digital satellite, digital cable, DRM-delivery to PCs, Telco TV and DVD and D-VHS packaged media all use content encryption and key management to protect content. Additionally, these systems use contractual mechanisms to require protection of content in accordance with compliance and robustness rules, e.g., product behavior and authorized outputs.[1]

As the MPAA observe: 'This sets Digital Broadcast TV apart from all other forms of digital content distribution as the only professional digital content distribution format that is unprotected.'[2] It is 'unprotected' because of the nature of free-to-air broadcasting previously described.

This creates a conundrum for social policy. Copyright owners, faced with the threat of unauthorised and uncontrollable Internet distribution of their content, may rationally seek to impose some form of control over whatever delivery means they elect, so as to prevent or inhibit that Internet distribution. However, the very nature of free-to-air broadcasting tends to make it problematic to consider how control could be imposed and also preserve its fundamental nature of being 'in the clear'; freely available to be apprehended by all within its footprint. If digital terrestrial broadcasting fails to include technological protection measures, any titles included in the digital broadcast are readily amenable to unauthorised Internet distribution. Therefore – at least under a prediction offered by the

---

[1] Jim C. Williams, 'Preserving the Viability of Digital Broadcast TV', a conference paper delivered on behalf of the MPAA at the Asia-Pacific Broadcasting Union's *DTV Symposium Digital TV – Challenges for the Broadcaster*, Kuala Lumpur, October 2005 and available at an attachment to a submission to the Australian government at http://www.dcita.gov.au/__data/assets/pdf_file/40122/Motion_Picture_Association_submission.pdf (last visited 16 May 2007), 2.

[2] Ibid

MPAA – copyright owners may become unwilling to licence those titles for free-to-air digital broadcast, preferring instead to limit distribution to one of the avenues offering control. If this were to occur, over time free-to-air broadcast content would diminish, as quality titles migrated to those protected platforms.

This chapter seeks to consider what has been put forward as one solution to this conundrum; broadcast flag technologies and their related regulations. These technologies and regulations seek to preserve the 'in the clear' nature of terrestrial broadcasting, while affording a degree of technical protection which is primarily directed to preventing uncontrollable, unauthorised Internet distribution.

Technology in the US, Europe and Japan

A broadcast flag is an electronic notice which is associated with a digital broadcast. The US implementation is its simplest form, comprising merely two bytes of information, which can be set as either 'on' or 'off' in respect of the associated broadcast.[3] The proposed European CPCM flag is far more elaborate. However, flags are not effective technological protection measures in the sense understood in copyright. As merely a piece of descriptive code embedded within a broadcast, flags do not *per se* lock, encrypt or scramble broadcasts prior to reception. Instead the code is merely a request that hardware receivers limit what can be done with the broadcast after reception.

Regulatory mandate of hardware compliance with a flag request is the consequence of this light-handed nature. This regulation is necessary for three inter-related reasons: (i) a flag does not effect technical exclusion, and therefore not only are legacy digital receivers not affected by it but there is no technical need for future equipment to obey it in order to receive the broadcast; (ii) hardware which ignores the flag has generally greater functionality than hardware which respects the flag; and, (iii) future suppliers of non-compliant equipment would have a competitive advantage over compliant suppliers. Thus, without legal mandate the whole exercise in applying a flag would be pointless.

The tightness of the relationship between the electronic notice that is the flag, and the regulations which mandate receiver compliance, has created confusing nomenclature. The term 'broadcast flag' has been applied in the US to both the electronic notice and the flag regulations promulgated in 2003 mandating hardware compliance. The MPAA has explained that the 'broadcast flag' term 'is used both for the rights usage signaling information that is placed in the unencrypted broadcast and for the regulation that gives it meaning'.[4] In this chapter, such confusing use of terminology will be avoided. The term 'flag' is used to refer only to the electronic notice, whereas the term 'mandate' is used to refer to public laws which require hardware to recognise the presence of a flag request. Taken together, a flag and its mandate is referred to as a 'regime'.

While the US and European broadcast flags share the same fundamental nature, they differ markedly in their modes of implementation. The US flag relies upon public law not

[3] Ibid 8.
[4] Ibid 8.

only to mandate hardware recognition but also to specify hardware behaviour. A future European CPCM flag will also need to rely upon public law to mandate hardware recognition. However once recognised, hardware behaviour is specified by the CPCM standard itself. The Japanese solution is of a different nature altogether. It is not a flag-based approach but relies instead upon encryption at the source. It will be considered by way of contrast with the more light-handed flag-based approaches.

US Broadcast Flag

The US flag is able to be included with the broadcast because the US digital television broadcast standard (devised by the Advanced Television Standards Committee) reserved a place – two bytes – in the signal for a 'redistribution control descriptor'.[5] This term conveys its primary objective: effecting control on the redistribution of digital broadcast content beyond the domestic environment. 'Beyond the domestic environment' includes most obviously 'the Internet'. As explained above, the broadcast flag as a technical component is essentially a simple piece of code which can be set as 'on or off'. Importantly, the flag alone does not effect any technical control. An 'on' setting only has effect to the extent receiving hardware is programmed or configured to respond. As observed above, it is how public law regulations mandate hardware to respond to the receipt of flagged content that effectively implements the flag's objective to technically control hardware behaviour. In other words, for the flag as an aspect of the broadcast standard to be effective, it requires hardware obedience which could only be ensured by complementary public law which mandates hardware behaviour once it has received a flagged broadcast. Therefore the US flag can not be meaningfully considered without describing this legal mandate which, given the simplicity of the electronic notice, serves as a complementary specification for digital receiving devices.

The joint proponents of the US flag legal mandate which was promulgated by the Federal Communication Commission (FCC) in 2003, included the MPAA, broadcast networks, certain consumer home electronics companies and certain technology companies.[6] The form of the hardware mandate can be properly regarded as a consensus position between these groups. The FCC flag mandate required that receiving devices made after 1 July 2005 should permit the electronic outputting of a flagged broadcast in one of six ways, summarised as follows:

1. In analog form;
2. In a form suitable for conventional cable or satellite retransmission provided the flag is retained;
3. In digital form to an authorized digital output technology;
4. In encrypted digital form to a product controlled by the receiver;
5. In encrypted digital form to an integrated recording device uniquely associated with the receiver;

[5] Ibid 8. For greater detail see: *In the Matter of: Digital Broadcast Content Protection*, 18 FCC Rcd 23550 (2003), 23556-23560.
[6] Thomas S. Fletcher, 'Charting the Future of Content Protection for Digital Television', (2006) 21 *Berkeley Technology Law Journal* 613, 621-625.

6. In a low-definition digital format when the receiver is incorporated in computing equipment.[7]

The objective of the mandate was to give legal consequence to the redistribution control descriptor (the flag) being 'on'. It is the mandate which provides the true source of control in respect of flagged content by regulating equipment suppliers; the flag *per se* does not effect technical control. To put it another way, control is *de jure* and not *de facto*.

Some features of this flag regime should be pointed out. First there is the so-called 'analogue hole'; the US flag regime does not seek to prevent analogue output being converted back into a digital format for Internet distribution. Second, the category of output – to 'authorized digital output technology' – are outputs which themselves require regulatory authorisation. In the only such FCC determination in 2005, several different copying technologies were approved, as were technologies which permitted the secure on-transmission to up to 10 devices uniquely associated with the outputting receiver.[8] The latter defined a type of 'authorised domain' (to use a term deployed in the CPCM system) of permitted digital re-distribution. Third, there is nothing in the mandate that requires that equipment receiving flagged broadcasts must limit the number of digital copies that can be made from the broadcast. Fourth, because the flag is merely a request included with an unencrypted broadcast, any appropriate receiver can technically render the flagged broadcast and output the digital feed in any form. This means the imposition of the flag is entirely consistent with the 'in the clear' nature of free-to-air broadcasting earlier described. Moreover it also means that the flag is 'backwards compatible'; it has no effect upon the operation of older, legacy digital receivers which are not capable of recognizing the flag.[9] The mandate did not require that legacy devices behave in any way on receipt of flagged content.

European CPCM System

A proposed European broadcast flag known as the CPCM system remains in a protracted gestation. Its provenance is with the Digital Video Broadcasting (DVB) Project, an industry consortium of broadcasters, consumer home electronics manufacturers, technology companies and regulators. It was formed in 1993 after industry failed to accept a European Commission supported, and EU mandated, digital satellite broadcasting standard.[10] Therefore, the DVB consortium can be seen as having its origins in a rejection of a bureaucratic, top-down imposition of technical standards. The CPCM

[7] *In the Matter of: Digital Broadcast Content Protection*, 18 FCC Rcd 23550 (2003), Appendix B.
[8] *In the Matter of: Digital Output Protection Technology and Recording Method Certifications*, 19 FCC Rcd 15876 (2004).
[9] Fletcher, above note 6, 617-618.
[10] Chris Hibbert, 'The DVB Approach to Content Protection & Copy Management', seminar paper delivered on behalf of the DVB consortium at the University of Melbourne Centre for Media and Communication Law's *The Future of Television: Legal Protection of Digital Broadcast Content – technology, Copyright, Law*, Sydney and Melbourne, 4 April 2007. See further Council Directive 92/38/EEC of 11 May 1992 on the adoption of standards for satellite broadcasting of television signals and the broader discussion in Carl Shapiro and Hal R. Varian, *Information Rules* (1999), 218-223.

system is an embryonic technical standard coming out of the consortium which is intended to apply to a plurality of content delivery modes – not only digital broadcasting. However, coming as it does from the DVB consortium, a primary driver appears to be digital broadcasting, and this chapter will primarily focus upon the CPCM system's broadcast applications. A descriptive specification known as the Reference Model was published in 2005, as part of the 'CPCM Bluebook',[11] and is currently in the process of being reduced to a technical specification for submission to the European Telecommunications Standards Institute (ETSI).[12]

The arrival at an industry-based consensus on the CPCM system was not straightforward. Chris Hibbert the Chairman of the DVB-Copy Protection Technologies Group, which was responsible for the formulation of the CPCM system, has explained that it took three years to merely arrive at the commercial (as opposed to technical) requirements for CPCM system.[13] The various interests were summarized by Hibbert along the following lines: copyright owners: 'to protect their revenues'; the consumer electronics industry: 'to protect the investment made by their customers in purchasing equipment and possible rejection of products which restrict content usage'; the public service broadcasters: 'concerned that signaling over-restrictive use of their broadcast content would conflict with their public service charters'; and pay TV broadcasters: 'looking for a means to integrate DVB-CPCM with existing conditional access systems to support new commercial offers such as push-VOD to PVR'.[14] The summary gives some flavour of the farrago of different positions that needed to be accommodated in the industry process.

Like the US broadcast flag, the CPCM system's predominate character is a concern to confine subsequent communications or transmissions of a received broadcast. This is achieved through CPCM-compliant devices respecting 'usage state information' (USI) coded within the digital medium. A critical aspect of the CPCM system is the flexibility and richness of the USI, which will reflect whatever usage rules have been set by the broadcaster or other relevant rights holder. A preface to the CPCM Bluebook is at pains to point out that:

> CPCM is designed to accommodate a variety of business models. The existence of any particular field of USI does not imply that it will be asserted by a particular business, or that it will be allowed to be asserted, or that a particular implementation will require the full functionality described in the Reference Model.[15]

The usage rules, being the particular settings that may be elected by the content provider, are categorized into five groupings: (i) copy and movement controls; (ii) consumption

---

[11] DVB Project, Content Protection & Copy Management, DVB Document A094, November 2005 ('CPCM Bluebook') available at http://www.dvb.org/technology/dvb-cpcm/a094.DVB-CPCM.pdf (last visited 16 May 2007). This publication includes within it other documents, including 'CPCM Reference Model SB1496' and 'Usage State Information (USI) SB1497'. These documents are paginated separately and will be referred to in notes below as 'CPCM Bluebook – Reference Model' and 'CPCM Bluebook – USI'.

[12] Hibbert, above note 10.

[13] Ibid.

[14] Ibid.

[15] CPCM Bluebook, above note 11, 'CPCM Compliance' Preface.

control; (iii) propagation control; (iv) output control, and, (v) ancillary control. Derived from the CPCM Bluebook, they are summarised below.

(i) Copy and Movement Control

These controls relate to traditionally the cardinal exercise of rights in copyright – to make a copy. The possible settings that can be applied to content are:

- No restriction on copying ('copy control not asserted').
- Exactly one copy allowable ('copy once') so that once a copy is created, no further copying would be allowed from it ('copy no more') except for a temporary buffer as described below for the copy never setting.
- No copies are allowed to be made ('copy never'), except for a secure temporary buffer copy solely for the purpose of pausing of play-back, or trick-play, where the buffer copy would be neither accessible to the user nor maintained longer than is necessary to provide the pause or trick-play function. [No buffering at all may be elected for content emanating from systems which provide their own pause or trick-play mechanism for the user, such as DVD, so that any subsequent cascaded pause function within the CPCM system would be unnecessary and might cause confusion for the user ('copy never, zero retention').]
- A move function which permits content to be transferred to another storage device ('move') but where such functionality is permitted it must comply with other usage restrictions. [For example, when the content carries a 'copy no more' setting then if moved to another storage medium the original copy must be no longer accessible.][16]

(ii) Consumption Control

Consumption is a term that is applied in the CPCM Reference Model (and USI) to mean the intelligible rendering of content on devices. These are devices which have received content from a copy of the broadcast. The possible settings that can be applied to content are:

- Time-based control, which would bar the consumption (intelligible rendering) or propagation (viewing, copying or movement within or beyond certain defined CPCM realms) of the content after a point in time. [This could be an absolute period (a specified date), or a period defined initial acquisition or consumption (X days after acquisition or consumption).]
- Usage control, which would limit the number of times content can be consumed (intelligibly rendered) or exported (released from the CPCM system).[17]

(iii) Propagation Control

[16] CPCM Bluebook – Reference Model, above note 11, 31-32.
[17] Ibid 32.

'Propagation' under the Reference Model (and USI) relates to the ability to intelligibly render the broadcast content within a defined realm. The CPCM system defines a variety of different realms within which certain propagation is permitted and facilitated. The possible settings that can be applied to content are:

- 'Restricted to authorised domain', which will permit outputting the content only to devices belongs to the authorised domain in which that cont was first acquired. [The authorised domain comprises CPCM-compliant devices controlled by members of a single household, defined in turn as 'the social unit consisting of all individuals who live together, as occupants of the same domicile'.]
- 'Restricted to local environment', which will permit outputting to devices in the immediate vicinity, assessed under a proximity test using a network tool used to measure the time it takes for electronic messages to pass between host points.
- 'Restricted to localised authorised domain', which permits outputting only to devices in both the authorised domain and the local environment. [A more specific area restriction is 'restricted to geographically constrained authorised domain' limited to devices which have the facility of verifying its geographic location.]
- 'Propagate to untrusted space' (ie unrestricted) so as to leave the realm of the CPCM system altogether. [Illustrative uses given for this setting included creative commons licensed material and promotional clips of commercial content.][18]

(iv) Output Control

'Output' refers to the release of content beyond a defined realm.

- For consumption output (ie in analogue form to devices in order to render the content intelligible to the human eye or ear) the possible settings that can be applied to content permit:
    1. Ability to enable and disable the output on analogue outputs for standard definition video;
    2. Ability to enable and disable the output on analogue outputs for high definition video;
    3. Ability to ensure that, if image constraint is signaled, resolution is constrained within specified parameters prior to high definition analogue output.
- For exported output (ie transmission outside the CPCM system) the possible settings that can be applied to content permit:
    1. Trusted export: a digital output to a trusted content protection system with no explicit control of the output.
    2. Controlled export: a digital output of content mapped to a trusted content protection system under the explicit control of usage rule.
    3. Untrusted export: a digital output or storage format that is neither trusted nor controlled.

[18] Ibid 29-30 and 33-36.

4. Analogue exported content: is an unprotected analogue output. [However such output may be subject to the copy control usage rules whereby content carrying the copy control states 'copy never' or 'copy no more' should not *become* analogue exported content.][19]

(v) Ancillary Control

A final setting is the ability to elect 'do not scramble' content which is transmitted under other rules within the CPCM system. Such scrambling (encryption) otherwise occurs to make more secure permitted propagation within the CPCM system.[20] European free-to-air broadcasters (who required this setting in the Reference Model) have indicated that they will define settings under the USI whereby post-reception content scrambling should not be applied. The only restrictions such broadcasters have indicated that they will select are those which inhibit the uncontrolled exporting of content for Internet communication – type (iv) above.[21]

It is apparent that the CPCM system is more elaborate and quite distinct from the two bytes of data signaling either 'on' or 'off' that comprises the US broadcast flag. However, notwithstanding its complexity, the CPCM system shares a fundamental characteristic with the US flag. It, like the US flag, does not lock, encrypt or scramble the broadcast prior to a point of reception. CPCM system is also based on merely a notice – albeit a notice, as shown above, with a far greater range of possible settings than merely 'on' or 'off'. But as merely a notice it does not self-enforce submission to the technology. Consistent with its fundamental flag nature, legacy digital receivers are unaffected by the presence of CPCM encoding.[22] Compelling the obedience of future hardware to the entire CPCM system must come ultimately, like the US broadcast flag, from public law.[23]

Japanese Source Encryption

An important comparison with these two models is the way in which Japan dealt with the issue in its free-to-air digital terrestrial broadcasting system. Japan uses the Integrated Service Digital Broadcasting (ISDB) standard which is essentially a common standard across the subscription digital satellite (ISDB-S) and free-to-air digital terrestrial (ISDB-T). It is this commonality which is critical in considering the copyright solution adopted

[19] Ibid 36-37 and CPCM Bluebook – USI, above note 11, 19-20
[20] CPCM Bluebook – Reference Model, above note 11, 37
[21] Hibbert, above note 10.
[22] In person, Chris Hibbert at the Melbourne seminar referred to at note 10 answered 'absolutely none' to the author's question 'what impact does the CPCM have on legacy digital receivers?' See also Andrew T Kenyon and Robin Wright, 'Television as Something Special? Content Control Technologies and Free-To-Air TV' (2006) 30 *Melbourne University Law Review* 338, 354.
[23] Cory Doctorow, 'Europe's Broadcast Flag The Digital Video Broadcasting Project Content Protection and Copy Management: a stealth attack on consumer rights and competition', an Electronic Frontier Foundation written submission to the UK House of Commons Culture, Media and Sport Select Committee inquiry into *Analogue Switch-off: A signal change in television*, 29 Septmber 2005 and available at http://www.eff.org/IP/DVB/dvb_critique.php (last visited 16 May 2007). Doctorow there observes: 'CPCM is not free-standing and capable of voluntary adoption by the private sector; it requires the force of law to be effective'.

for the latter. In Japan, free-to-air broadcast is encrypted before transmission using the same conditional access system used for digital subscription satellite.[24] While access to the digital terrestrial broadcasts are without-charge (other than the general obligation, applicable for households with analogue or digital reception equipment, to enter into a receiver contract with the national Japanese broadcasting organisation, NHK) digital receivers decrypt the signal using an integrated circuit embedded in an conditional access card (known as the 'B-CAS').[25] In Japan digital broadcast receivers are supplied with the cards, which must be inserted for the reception equipment to render digital broadcasts intelligibly.[26] After decryption broadcasts of the major free-to-air broadcasters are encoded as 'Copy One Generation' and 'No Redistribution beyond the Home'. The 'Copy One Generation' controls have been explained in consumer-information published by the Japanese government in these terms:

> Because with the copying of digital information the sound and picture quality does not deteriorate, a protective measure has been incorporated to protect copyright and prevent illegal copying. This is being only able to make one copy (copy once). Any digital TV recorded under 'copy once' will not be able to be copied by other digital recorders. (Copies can be made with analogue recorders) However, data can be moved from hard disk to other recording media. If your recorder is equipped with 'move' capability, then recorded programs can be moved to other media. This process deletes the original recording. Example: A program recorded onto a hard disk can be moved to a DVD, but the original recording on the hard disk will be automatically deleted.[27]

These copy-controls have been the subject of controversy, and there has been suggestion that they may be relaxed.[28] Apparently less controversial are the 'No Redistribution beyond the Home' controls which entail the following four proprietary technological protection system technologies:

- Analog video outputs must have analog Copy Generation Management System (CGMS-A) rights signaling applied;
- Uncompressed digital display outputs are restricted with high-bandwidth digital content protection (HDCP);
- Compressed digital recording outputs are restricted with digital transmission content protection (DTCP), and,
- DVD recordings must be protected with content protection for recordable media (CPRM).[29]

---

[24] Williams, above note 1, 6-8. See for greater detail: Hiroshi Asami, 'Digital Broadcasting in Japan HDTV and Mobile Reception As Key Applications', a Japanese government official's conference paper delivered at Broadcast Asia 12 May 2005 and available at http://www.broadcastpapers.com/whitepapers/BAsia04MPHPTJapanHDTV.pdf (last visited 16 May 2007).
[25] Williams, above note 1, 6-8.
[26] Asami, above note 24, 7.
[27] Ministry of Internal Affairs and Communications/The Association for Promotion of Digital Broadcasting, 'The Quick Guide to Understanding Terrestrial Digital Television vol 3', April 2007, 10 and available at http://www.soumu.go.jp/joho_tsusin/dtv/pamphlet/pdf/hayawakari_en_vol3.pdf (last visited 16 May 2007).
[28] Masaharu Tanaka, 'Shift to Multiple Copies for a Single Generation Confirmed for Copy Once Technologies; Focus Now on Number of Copies' *TechOn*, 19 Apr 2007 available at http://techon.nikkeibp.co.jp/english/NEWS_EN/20070419/131207/ (last visited 16 May 2007).
[29] Williams, above note 1, 6.

Critically there seems to be in Japan no specific technological mandate in public law which requires hardware compliance with these restrictions. Rather the use of encryption-supported conditional access technology controls the platform, and more tightly compels hardware obedience with these copyright-control settings. A distinction can be readily observed. The Japanese model technically protects broadcasts at the source and receivers are therefore technically obliged to obey the encoded conditions. Flag models rely upon obedient hardware to technically protect broadcasts post reception and rely upon specific legal mandate to ensure that obedience.

Broadcasting law in US, Europe and Australia

One consequence of the looseness of the flag-technologies as copyright-control mechanisms is that they have the political appeal of backward compatibility. Legacy devices are unaffected. But another consequence is that their efficacy requires a public law mandate directed at *subsequent* equipment manufacturers.

US Law

As noted above, in 2003 a Federal Communications Commission (FCC) rule-making represented such a hardware mandate.[30] It required that from 1 July 2005, all digital broadcast reception equipment sold in the US must obey the six output constraints described above, one of which was defined in a subsequent 2005 determination which permitted limited and secure digital redistribution to a finite number of devices.[31] In this way, once flagged broadcasts are transmitted into a future world populated exclusively with the mandated hardware, there is no easy way that digital broadcast content *per se* can be retransmitted or otherwise made available on the Internet by the notorious 'guy sitting in his living room in his pajamas'.[32] All his receivers will deny him the ability to output the broadcast in digital high definition format suitable for peer-to-peer, Bittorent, YouTube or whatever other indiscriminate redistribution medium he chooses. The best he can do is to avail himself of the analogue hole or use the permitted lower-definition digital output from his computer's digital receiver.

In 2005, shortly before they were to come into effect, the US Court of Appeals for the District of Columbia Circuit struck down the FCC regulations as *ultra vires*.[33] The Communications Act provision relied upon by the FCC was construed as a power to regulate devices for the technical process of transmission and reception. The flag regulations were correctly understood by the Court to relate to the behaviour of devices after the broadcast had been technically received.[34] In response to this decision, the joint

[30] *In the Matter of: Digital Broadcast Content Protection*, 18 FCC Rcd 23550 (2003).
[31] *In the Matter of: Digital Output Protection Technology and Recording Method Certifications*, 19 FCC Rcd 15876 (2004).
[32] This was a character identified in the blogging context by Jonathan Klein, a former CBS executive: Howard Kurtz, 'After Blogs Got Hits, CBS Got a Black Eye', *Washington Post*, 20 September 2004 and available at http://www.washingtonpost.com/wp-dyn/articles/A34153-2004Sep19.html (last visited 16 May 2007).
[33] *American Library Association v FCC*, 406 F 3d 689 (DC Cir, 2005).
[34] Ibid 699-700.

proponents of the flag sought legislative reform to confer power upon the FCC to make valid flag regulations. To date, these efforts have been unsuccessful. This has been in part due to complications arising from interests associated with the US sound recording industry to ensure legislative power to promulgate regulations for a future, unspecified, audio flag. It seems unlikely that there will be US legislative reform of any sort before the next congressional elections in 2008.

European Law

It is unclear by what means the CPCM system would be mandated in Europe. It is clear from the terms of the 2001 *Information Society Directive* that specific technological mandates were not to be favoured for technological protection measures in copyright law.[35] An alternative avenue might have been the revision which is currently underway to the 1989 *Television Without Frontiers Directive*.[36] The revised directive, renamed the *Audiovisual Media Services Directive*, proposes largely consumer-protection orientated rules for broadcasters. Although at one point a recital in the most recent draft descends into the realm of copyright (seeking to ensure access to short extracts for reportage) it appears unlikely that this directive would ultimately include any provisions which relate to a CPCM flag mandate.[37] The present literature from the DVB consortium is laconic as to the precise legal means by which the CPCM system would be mandated in Europe.

An interesting point of possible distinction between the US and European flag arises from the differing extent of regulatory control between the two. The US flag's meaning in terms of control is defined by public law. The technology simply signals 'on' or 'off'. In Europe this could be somewhat reversed. The proposed European flag's meaning in terms of control is defined by that selectable within the five CPCM system control genres; these are technical settings. If European law were to simply require the supply of CPCM-compliant hardware after a certain date, it would be the broadcaster (or rights holder) who would be making the choice from the possible settings. This scenario was derided by Cory Doctorow of the Electronic Frontier Foundation (EFF) in a submission to a UK Parliamentary committee:

> In effect, CPCM and its constituent specifications amount to a complicated, lengthy, and, at present, secret body of private law that describes rules and restrictions potentially applicable to all manufacturers of DTV devices. It is already clear that at least some CPCM coauthors expect -- and require -- the co-operation of regulators to make this scheme obligatory upon these manufacturers.[38]

---

[35] Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, chapter III.
[36] Council Directive 1989/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities.
[37] European Commission, Draft Audiovisual Media Services Directive, Non Binding Working Document rev 3, April 2007 available at http://ec.europa.eu/avpolicy/docs/reg/modernisation/proposal_2005/avmsd_cons_amend_0307_en.pdf (last visited 16 May 2007).
[38] Doctorow, above note 23 (reference omitted).

A competing view was that the 'finely granulated control made possible by the CPCM system may provide additional regulatory possibilities for the protection of exceptions to copyright'.[39] This view imagines that any hardware compliance mandate could be coupled with regulations directed against broadcasters (and presumably other rights holders) that encodes content with CPCM restrictions:

> It seems that with CPCM, regulators could seek to prevent certain USI from being applied to particular areas of control — such as copy and movement control, consumption control or propagation control — and this could be done in relation to all or certain types of content.[40]

A similar type of point was raised before the FCC. Should broadcasters be given complete discretion as to whether they switch the flag on, or should FCC regulations fetter that choice? Public interest groups had submitted that any FCC rule-making should include 'a prohibition on use of the flag for news and public interest programming'.[41] The FCC disagreed, preferring flag election to be a purely commercial matter for the broadcaster.[42] While it remains to be seen what shape (if any) European law takes in this area, it certainly appears that the proponents of the CPCM system are not envisaging regulations which extend beyond a straightforward hardware compliance mandate.

Australian Law

The Australian *Broadcasting Services Act* (BSA) provides as a cardinal, defining obligation, that commercial broadcasting services licensed to use the spectrum must provide programs that are 'able to be received on commonly available equipment' and 'made available free to the general public'.[43]

In 2000 digital television broadcasting was regulated in the BSA. From that time, and as a condition of their licences, broadcasters were to comply with any regulation made by the body now known as the Australian Communications and Media Authority (ACMA), which ensured that they entered into no 'agreement, arrangement or understanding' in relation to the provision of domestic digital receivers unless those receivers are 'accessible by' all other broadcasters.[44] No such regulations have been made, and any such regulations would have been directed not at the suppliers of receiver hardware but rather licensee broadcasters who may have had dealings with those suppliers. As a legislative regime it would have been incapable of mandating hardware compliance with any future Australian broadcast flag.

---

[39] Kenyon and Wright, above note 22, 354.
[40] Ibid 358.
[41] *In the Matter of: Digital Broadcast Content Protection*, 18 FCC Rcd 23550 (2003), 23568.
[42] Ibid 23568-23569.
[43] *Broadcasting Services Act* 1992 (Cth), section 14 (b).
[44] *Broadcasting Services Act* 1992 (Cth), Schedule 2, Standard Conditions Part 3, clause 7(1)(oa): 'the licensee will comply with any regulations made for the purposes of clause 36B of Schedule 4', where clause 36B deals with licensee agreements relating to the accessibility of domestic reception equipment. Clause 7(1)(oa) was reformed upon commencement of new Parts 9A and 9B.

This has been addressed as part of a swag of broadcasting law reforms that were made late 2006 and came into force early May 2007.[45] A new Part 9A of the BSA confers on ACMA the power to make regulations setting the technical standards that relate to digital broadcasts and domestic reception equipment that is capable of receiving those digital broadcasts. The Part creates an offence and a civil penalty for those who supply equipment which is 'capable of receiving' digital broadcasts, but does not comply with any regulated technical standards.[46] Apart from technical standards, ACMA is given power to determine regulated 'industry standards' under new BSA Part 9B. That Part includes gives ACMA the power to determine what 'sections of the industry' are, and to prescribe industry standards which extend to anyone who is a 'participant in a section of the industry'.[47] Prescribed industry standards are intended to augment or bolster any existing voluntary industry codes, and prescribed industry standards made under Part 9B may not deal with matters of technical standards that are made under Part 9A.[48] The scope of prescribed industry standards which might be made is illustrated by a list which includes the labeling of domestic reception equipment.[49] It would therefore seem that hardware receiver suppliers fall within the concept of 'participants in a section of the industry'.

Is ACMA empowered under the reforms to mandate the supply in Australia of only flag-compliant receivers? It seems that if such a power does not exist under the technical standards provisions under Part 9A for reasons similar to those suggested by the DC Circuit Court of Appeals, the power almost certainly would exist under the industry standards provisions of Part 9B.

The WIPO Broadcasters' Treaty

The updating of broadcasting organization protection has been discussed for some time within the World Intellectual Property Organization (WIPO). Broadcaster's protection was omitted from the updating of copyright, performers' and sound recording producers' rights in a pair of 1996 treaties (1996 WIPO treaties).[50] Drafts of a new WIPO Treaty on the Protection of Broadcasting Organizations (Broadcasters' Treaty) have been

---

[45] *Broadcasting Legislation Amendment (Digital Television) Act* 2006, section 2.
[46] *Broadcasting Services Act* 1992 (Cth), section 130B(2).
[47] *Broadcasting Services Act* 1992 (Cth), sections 130G, 130H and 130V.
[48] *Broadcasting Services Act* 1992 (Cth), sections 130L(c) and 130R-U.
[49] *Broadcasting Services Act* 1992 (Cth), section 130K(3)(a). Of interest in the context of the issue of copyright in program guides another possible area of industry standard-making is 'the provision of information for the purpose of compiling electronic program guides': section 130K(3)(b).
[50] WIPO Copyright Treaty, opened for signature 20 December 1996, 36 ILM 65 entered into force 6 March 2002; WIPO Performances and Phonograms Treaty, opened for signature 20 December 1996, 36 ILM 76, entered into force 20 May 2002. On 26 April 2007 (the World Intellectual Property Day for 2007) the Australian government deposited its instruments of accession to the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty, both treaties coming into force for Australia on 26 July 2007. See government press release: http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/AllDocs/E8AC29AB4FF5A19FCA2572C9000F9A17?OpenDocument (last visited 16 May 2007). The binding date for each Treaty is three months from the deposit of instrument of accession: WIPO Copyright Treaty, art 21(ii) and WIPO Performances and Phonograms Treaty, article 30(ii).

circulating within WIPO since early June of 2004.[51] To what extent are flag technologies and mandates being considered within the treaty-making processes? The answer seems to be, not much. There is certainly nothing in the most recent official draft of July 2006 which imposes an obligation of mandating, in national public law, hardware compliance with a broadcast flag.[52] It is also clear enough that broadcast flags do not fall within the concept of an 'effective technological protection measure' (ETPM), a concept previously deployed in the 1996 WIPO treaties.[53] Unlike the Japanese system, flags provide no 'effective' technological protection in and of themselves. They do not need to be circumvented to access or copy or redistribute the broadcast – unless mere disobedience was considered circumvention, which it manifestly is not. What flags provide is a technical standard for which the law can mandate a degree of equipment compliance. However the July 2006 draft may address broadcast flag technologies in another way. Flags, or at least certain flags, may be regarded, instead, as a type of 'electronic rights management information' (ERMI), also protected in the 1996 WIPO treaties and proposed to be similarly protected under the July 2006 Broadcasters' Treaty draft. However under these provisions ERMI is protected only against removal or alteration.[54] That is, there is no obligation to ensure obedience to ERMI. ERMI is defined in the July 2006 draft as:

> information which identifies the broadcasting organization, the broadcast, the owner of any right in the broadcast, or information about the terms and conditions of use of the broadcast, and any numbers or codes that represent such information, when any of these items of information is attached to or associated with (1) the broadcast or the signal prior to broadcast, (2) the retransmission, (3) transmission following fixation of the broadcast, (4) the making available of a fixed broadcast, or (5) a copy of a fixed broadcast.[55]

Because this definition requires 'information about the terms and conditions of use of the broadcast' it raises the interesting question whether the 'on' or 'off' two bytes of data which comprises the US broadcast flag could qualify under this definition, or whether such simple binary data would be too insubstantial to qualify. This chapter offers no answer to that question, other than to observe that the source of the terms and conditions resides not so much in the data itself, but in the FCC regulations which give the 'on' designation meaning. In contrast it may be less ambiguous that the detailed settings of the CPCM system could comprise ERMI information of this sort, providing as it does in code, the substantive terms and conditions of the broadcast's use.

In the first half of 2007 WIPO published a pair of non-papers which proposed further revision to the July 2006 draft treaty. These were prepared in an attempt to reconcile quite divergent national views on the extent to which the Broadcasters' Treaty should

---

[51] Consolidated Text for a Treaty on the Protection of Broadcasting Organizations, SCCR/11/3, 29 February 2004: http://www.wipo.int/edocs/mdocs/copyright/en/sccr_11/sccr_11_3.pdf (last visited 16 May 2007).
[52] Revised Draft Basic Proposal for the WIPO Treaty on the Protection of Broadcasting Organizations, SCCR/15/2, 31 July 2006: http://www.wipo.int/edocs/mdocs/sccr/en/sccr_15/sccr_15_2.pdf (last visited 16 May 2007).
[53] Ibid 72-74 (proposals relating to article 19).
[54] Ibid 77 (proposed article 20(1)).
[55] Ibid 77 (proposed article 20(2)).

reflect public interest concerns as opposed to the private interests of broadcasting organizations. The papers proposed a scaling back of protection to a so-called 'signal-based' approach.[56] In these non-papers the ETPM and ERMI protections were made less detailed. The most recent of the two non-papers – dated April 2007 – simply suggests the following:

> Contracting Parties shall provide adequate and effective legal protection against unauthorized
> (i) decryption of an encrypted broadcast, or circumvention of any technological protection measure having the same effect as encryption;
> (ii) manufacture, importation, sale or any other act that makes available a device or system capable of decrypting an encrypted broadcast; and
> (iii) removal or alteration of any electronic rights management information used for the application of the protection of the broadcasting organizations.[57]

Clearly, flags applied prior to broadcast do not encrypt the broadcast, nor are they measures which have 'the same effect as encryption'.[58] However paragraphs (i) and (ii) seem to afford an obligation on a country such as Japan to ensure that its encrypted digital terrestrial broadcasts are protected from circumvention. The non-paper drafts leave ERMI undefined, however if the definition in the July 2006 draft were to apply, the April non-paper's terms would provide the same sort of flag protection as the July 2006 draft; protection to a flag which qualifies as ERMI against its removal or alteration, but no obligation to ensure obedience.

The trajectory of the treaty-making process is uncertain. A note which prefaces the April 2007 non-paper explains that:

> The task of the preparation of a new non-paper has been complex because the opinions and comments expressed by the delegations diverge greatly, and in many cases point to opposite directions.[59]

Needless to say that these are hardly inspiring words to anyone who is enthusiastic about seeing a concluded Broadcasters' Treaty in the near-term.[60]

---

[56] Draft Non-paper on the WIPO Treaty on the Protection of Broadcasting Organizations, Draft 1.0, 8 March 2007 available at http://www.wipo.int/edocs/mdocs/sccr/en/sccr_s2/sccr_s2_paper1.pdf (last visited 16 May 2007) and Non-paper on the WIPO Treaty on the Protection of Broadcasting Organizations, 20 April 2007 available at http://www.wipo.int/edocs/mdocs/sccr/en/sccr_s1/sccr_s1_www_75352.doc (last visited 16 May 2007).

[57] Proposed article 9 in the non-paper on the WIPO Treaty on the Protection of Broadcasting Organizations, 20 April 2007 available at http://www.wipo.int/edocs/mdocs/sccr/en/sccr_s1/sccr_s1_www_75352.doc (last visited 16 May 2007).

[58] Notably the Australia–United States Free Trade Agreement 18 May 2004 [2004] ATNIA 5, article 17.7 creates with an obligation to create liability for the circumvention of encrypted satellite broadcasts. Australia has given effect to this obligation in a technologically neutral way by extending protection from circumvention to all subscription and most encrypted broadcasts: *Copyright Act* 1968 (Cth), Part VAA.

[59] Non-paper on the WIPO Treaty on the Protection of Broadcasting Organizations, 20 April 2007, 3 available at http://www.wipo.int/edocs/mdocs/sccr/en/sccr_s1/sccr_s1_www_75352.doc (last visited 16 May 2007)

[60] A subsequent WIPO meeting of the Standing Committee on Copyright and Related Rights in June 2007 failed to achieve agreement on the terms of a proposed Broadcasters' Treaty for a future diplomatic conference. Consequently the timetable remains stalled: WIPO Press Release PR/498/2007, 'Negotiators

Conclusions

As foreshadowed in the introduction, the crucial argument made by the content owners, including the MPAA, supporting the flag regime as good broadcast policy relates to the choice that producers of professional audio-visual content face in the absence of a flag regime. They can release their content in digital format for free-to-air broadcasting in circumstances under which that content is amenable to uncontrollable and unauthorised Internet distribution, or they can refuse to deal with that medium and distribute their content along other technologically protected channels which are buttressed by anti-circumvention copyright laws. Under the second option free-to-air broadcast viewers would end up with second-rate content. One striking thing about this argument – which was essentially accepted by the FCC – is the assumption about the power of the MPAA and other content owners to deny free-to-air broadcasters content and to distribute that content through other channels. The MPAA can be understood as saying that, over time, 'broadcasters need our content more than the MPAA needs the broadcasters' medium'. The reason this statement seems plausible to policy-makers is that broadcasting can be more and more seen to be just one of an increasing number of technological pathways down which a copyright producer could make content available. It is this more than anything else that gave the broadcast flag policy traction in the US.[61] If CPCM proponents succeed in attracting European regulatory mandates, this reasoning will be a central policy justification, although the CPCM system can also be seen to facilitate certain uses within the so-called authorised domain, and permits free-to-air broadcasters to place a bar on post-reception encryption.

Another thing implicit in the central MPAA argument is that no policy-maker would so derogate from the copyright owner's exclusive rights as to compel content to be licensed for free-to-air digital broadcasting. This assumption, while probably sound in the US, may not be so sound in other territories. Since 1928 a remunerated exception recognized in international copyright law permits the creation of a copyright exception for broadcasting so long as payment of a fair royalty to the rights holder is guaranteed.[62] One thing that could be considered is the possible future utilization of this flexibility in territories where digital broadcasting occurs and relevant copyright interests have less political power.

In Australia free-to-air broadcasters have more political power than audio-visual content providers. However the condition that was a key driver of the flag regime in the US – the power of the MPAA – could be felt through the influence of the MPAA on US trade policy. It is possible to imagine a day when the US Congress finally has put the FCC on a solid legislative footing to promulgate a valid flag mandate. Not long after that day it is also imaginable the US may attempt to export its broadcast flag regime to Australia

---

Decide to Continue Discussions on Updating Protection of Broadcasting Organizations', Geneva, 25 June 2007.

[61] *In the Matter of: Digital Broadcast Content Protection*, 18 FCC Rcd 23550 (2003) at 23555 observing that a flag mandate 'will ensure the continued availability of high value DTV content to consumers'.

[62] See generally David J. Brennan, *Retransmission and US Compliance with TRIPS* (2003), chapter 2.

through a round of Free Trade Agreement revisions. (From a US trade perspective it does make sense to export; there is no point having flag mandates in place in the US if the same high-definition broadcast content can be easily made available on the Internet by the 'Aussie sitting in his living room in his pajamas'.) If this was to occur the obligation would be likely to mirror whatever the US had in place and would perhaps be implemented here (and in other DVB digital broadcasting standard countries) by mandating hardware obedience with those aspects of the CPCM flag that corresponded with the protected US flag. This might particularly focus upon the fourth type of CPCM settings, output controls. In any event, the Australian legislative framework does now appear to be in place for ACMA to make such regulations under either Part 9A or Part 9B of the *Broadcasting Services Act*.

At the other extreme from this scenario is the position of the EFF, which is a non-government organization whose slogan dedicates it to 'defending freedom in the digital world'. The EFF submissions to the FCC against the US flag mandate included (1) that the flag was such a weak technological measure it was best described as a sieve,[63] but (2) that it will also damage legitimate, noninfringing activities.[64] These were mutually exclusive positions argued cumulatively. The EFF position on flag technologies, as it is with any like issue, is that as a matter of public policy copyright should always yield to technology. This is highlighted in the solution proposed by the EFF:

> [I]f consumer broadband bandwidth were to increase, content owners could obtain additional protection for their DTV broadcast content by requiring that broadcasters transmit in higher resolution formats … If consumer broadband capacities were to increase in the future, [a broadcaster] could begin broadcasting at higher resolutions, making it more difficult to redistribute the full-resolution content via the Internet.[65]

In other words, all that is required is to let broadcasters compete with unauthorised Internet distribution in a high-definition arms race; a kind of 'law of the digital jungle solution'.

Good arguments could be made that flag regimes best belong either within a copyright/rights of broadcasting organizations policy framework or within a broadcasting law policy framework. Flag mandates have the flavour of public law, rather than private law creating private rights. In this respect they are more akin to traditional broadcasting law rather than copyright/rights of broadcasting organizations law. But this is not to say that flag mandates are unrelated to copyright. For while flag mandates may be public rather than private law, it is public law which exists in the shadow of the emerging norm of generic protection for technological protection measures in copyright – a point well-made by the MPAA.

---

[63] Reply Comments of the Electronic Frontier Foundation in the Matter of Digital Broadcast Copy Protection, MB Docket No. 02-230, 18 February 2003, 8.
[64] Comments of Electronic Frontier Foundation in the Matter of Digital Broadcast Copy Protection, MB Docket No. 02-230, 6 December 2002, 13.
[65] Reply Comments of the Electronic Frontier Foundation in the Matter of Digital Broadcast Copy Protection, MB Docket No. 02-230, 18 February 2003, 18.

Which ever way flag mandates are considered, one striking thing about them is what technologically-specific law they are.[66] In this respect, flag mandates have a somewhat similar nature to a little-discussed provision in the 1998 Digital Millennium Copyright Act (DMCA). This provision effectively mandated the patented Macrovision copy-protection technologies, requiring that all video cassette recorders sold into the US market eighteen months after the DMCA's enactment had to obey the serial copying Macrovision controls which applied to many analogue pre-recorded videocassettes.[67] The underlying drafting philosophy of this provision – enacting specific technology mandates – was rejected for the 1996 WIPO treaties which preferred such protection to be couched in technologically neutral terms. This can be seen in the related European and Australian developments since those treaties. Specific technology mandates have not been enacted; rather laws have been couched in terms of protection to generic technologies which have copyright-control effects. This has become an article of faith in policy makers, keen not to be interfering with market processes by picking certain technologies over others. If flag mandates emerge as a part of public law, they can be seen as belonging to a type of highly-specific technology mandate akin to the DMCA's Macrovision laws of 1998. It is a type of law-making which has been largely rejected for the copyright system.

Given that the Japanese digital free-to-air encryption solution appears to be unique to that nation's technological, geographic and cultural circumstances, the question remains elsewhere how the law should provide for flag technologies, if at all. Accepting the policy argument for some form of technological protection on digital free-to-air-broadcasting, flag technologies do have appeal as being sufficiently light-handed to be accommodated within the open nature of free-to-air broadcasting. However, technology-specific and industry-specific mandates have an ugly 'command economy' feel. A slightly alternative approach might rely more on copyright and regard some flag-based systems (such as the CPCM) as a 'special type of ERMI' (SERMI). This would only occur once a specialist decision-making body, such as the US Copyright Office, was satisfied after a hearing that: (i) particular ERMI comprises an industry standard and it is reasonable in light of public policy; (ii) if patented technologies are involved, they will be licensed on public, fair and non-discriminatory terms; and, (iii) equipment obedience can be specified and implementing that obedience will involve minimal cost and inconvenience to manufacturers.[68] Once these criteria were satisfied, a rule-making could declare the particular ERMI to be SERMI. This would have the consequence that suppliers of the implicated equipment must ensure that it technically obeys the conditions contained in the SERMI from a particular date. Enabling legislation could require such regulation to be limited for a finite number of years, to ensure that the obligation to obey an aging SERMI is periodically reassessed. Needless to say, this approach necessarily entails a mandate for otherwise the whole exercise in applying a flag to digital content would be tokenism. However it is a more generic approach which arguably permits greater policy nuance, being not based on a specific industry. The CPCM system, for

[66] A point well-made previously: Susan P Crawford, 'The Biology of the Broadcast Flag' (2003) 25 *Hastings Communications and Entertainment Law Journal* 599, 651-652.
[67] Copyright Act 1976 (US), § 1201(k).
[68] Compare the powers that are conferred on the Copyright Office in promulgating exceptions to access control circumvention liability: Copyright Act 1976 (US), § 1201(a)(B)-(D).

example, has been created to be applied across a plurality of digital media. A legal approach such as the one suggested will mirror the broad-based nature of such a measure, and is more in keeping with the neutral treatment of such technical measures in copyright law.