



Australian Government

Attorney-General's Department

PROTECTING SUBSCRIPTION BROADCASTS

**Policy review concerning unauthorised access to and use of
subscription broadcasts**

Discussion Paper

May 2005

Index

Overview	2
1.Introduction	4
2.The subscription broadcast industry, services and concerns	8
The subscription broadcast industry	8
Services provided by the subscription broadcast industry	8
Unauthorised access to and use of a subscription broadcast.....	10
Impacts of unauthorised activities	13
Emerging technology affecting subscription broadcasts	14
3.Relevant criminal law and policy	15
When is conduct criminal in nature?	15
Model Criminal Code Committee examination of theft and fraud offences.....	16
Theft and fraud offences in State and Territory legislation	18
Theft and fraud offences in Commonwealth legislation.....	21
Effect of a criminal conviction	22
4.Unauthorised access and use not covered by the Copyright Act and the issue of criminalisation	24
Unauthorised access to and use of a subscription broadcast in the home.....	24
Other unauthorised activities concerning subscription broadcasts	32
Appendix 1 - Protection for subscription broadcasts under the Copyright Act	38
Copyright owners' rights	38
Use of copyright material	39
Enforcement of copyright	39
The Digital Agenda amendments	40
Amendments implementing the Australia-United States Free Trade Agreement.....	42
Appendix 2 - Current criminal offences and civil remedies in the Copyright Act concerning subscription broadcasts	43

Overview

The Government is reviewing whether various activities involving unauthorised access to and use of subscription broadcasts that are not currently criminal offences under Commonwealth law, ought to be made offences. In this context the term ‘unauthorised’ means that these activities are carried out without the authorisation of the subscription broadcast provider.

This paper has been prepared by the Attorney-General’s Department (the Department) for the purpose of inviting submissions to be made on the questions asked in the paper so that interested persons have the opportunity to ensure that the Government has all relevant views to consider as part of the review. The Government also welcomes comments on any other issue raised by the paper.

Section 1 of the paper provides the general background to this review. Section 2 provides information on the subscription broadcast industry and outlines concerns raised by the industry relating to current Government policy on the unauthorised access to and use of subscription broadcasts. Section 3 provides a discussion of relevant criminal law and policy. Section 4 outlines various activities relating to subscription broadcasts that are not currently regulated under Commonwealth law and competing arguments for criminalisation of those activities. It includes specific questions on which comments are sought.

Appendix 1 sets out the current protection for subscription broadcasts under the *Copyright Act 1968*. A table summarising the current offences and civil remedies in the Copyright Act in relation to encoded broadcasts is in Appendix 2.

Submissions should be made by **17 June 2005** and should be addressed to:

Ms Helen Daniels
Assistant Secretary
Copyright Law Branch
Attorney-General’s Department
Robert Garran Offices
National Circuit
BARTON ACT 2600

It would be appreciated if submissions could be provided electronically by email to copyrightlawbranch@ag.gov.au. Questions concerning this review may be directed to Gabrielle Mackey by email at gabrielle.mackey@ag.gov.au or by telephone 02 6250 6608, or facsimile 02 6250 5929.

Submissions may be made public on the Attorney-General's Department website unless otherwise specified. Persons providing a submission should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available. Copies of submissions may be made available to other Commonwealth Government agencies with an interest in this review.

1. Introduction

1. The first subscription broadcast television (TV) service in Australia commenced broadcasting in January 1995.¹ Since then the subscription broadcast industry in Australia has grown steadily. For example, FOXTEL commenced its cable service in October 1995 with 20 channels. In March 2004 it launched its new digital service with 130 channels.² There are now approximately 1.6 million Australian homes with subscription broadcast services with a viewing potential of 5 million people.³

2. A broadcast, whether a free-to-air or subscription broadcast, is covered by copyright in Australia. The broadcaster is the copyright owner. Unless the broadcast is a live broadcast there will generally also be separate copyright rights regarding the content of the broadcast (such as pre-recorded programs, films, scripts and soundtracks). There are usually separate copyright owners of these copyright rights.

3. Copyright owners sometimes use technological means to protect their copyright material. Encrypting a broadcast so that only persons who have been supplied with a decrypting device can access the broadcast is a means by which broadcasters can protect their copyright and any copyright that applies to the content of the broadcast. Supplying persons who have subscribed to a subscription broadcast service with the necessary equipment to receive and decode the broadcast is the means by which subscription broadcast providers protect their product and their business.

4. Specific protection for subscription broadcasts is found in the *Copyright Act 1968* (Copyright Act). Relevant provisions in the Copyright Act refer to an 'encoded broadcast' which may be made by a commercial or national broadcasting service. As the issues raised in this paper concern various activities involving unauthorised access to and use of encoded broadcasts which primarily relate to the industry that provides subscription broadcast services, the term

¹ The first service, Australis (operating as Galaxy) began in January 1995 and was followed by AUSTAR (August 1995), OPTUS VISION (September 1995) and FOXTEL (October 1995). [Source: History of Subscription TV: <http://www.astra.org.au/article.asp?section=2&option=1&content=2>]

² Information obtained from FOXTEL website [<http://www.foxtel.com.au/>] January 2005.

³ FOXTEL and AUSTAR have been reported to have 1.4 million subscriber households between them and FOXTEL is adding about 12,000 digital subscriptions a week: *The Australian*, Article by Lara Sinclair, 'Pay-TV audience figures disputed', Nov 11, 2004.

‘subscription broadcast’ has often been used in preference to the broader term ‘encoded broadcast’. For the purposes of this paper they mean the same thing.

5. The Copyright Act was amended in 2001 to provide civil remedies and criminal offences in relation to the manufacture, importation, sale and other dealings with ‘broadcast decoding devices’ that facilitate unauthorised access to subscription broadcasts.⁴ The range of civil remedies and criminal offences was extended in January 2005 when amendments to implement obligations under the Australia-United States Free Trade Agreement (AUSFTA) came into effect.

6. This paper assumes that the reader has a general understanding of how copyright is currently protected in Australia, how broadcasts and the content of broadcasts are protected and the provisions of the Copyright Act that assist copyright owners to enforce their copyright. For the benefit of those readers who may not have this understanding, relevant information is contained in Appendix 1. A table summarising the current offences and civil remedies in the Copyright Act in relation to encoded broadcasts is in Appendix 2.

7. The Copyright Act does not criminalise or provide civil remedies for all unauthorised activities concerning broadcast decoding devices, or unauthorised access to or use of subscription broadcasts more generally. In some cases this results from the way in which the legislative provisions have been structured. In other cases, notably situations concerning private and domestic access and use, this has been a deliberate policy approach. To date the Government’s policy has been that the main focus for public law enforcement should be on the acts of those who provide the means by which the unauthorised activity is conducted or who profit from that activity.

⁴ The relevant amendments were made by the *Copyright Amendment (Digital Agenda) Act 2000*. The term ‘broadcast decoding device’ is defined in section 135AL of the Copyright Act.

8. The wording ‘unauthorised access to and use of’ subscription broadcast services has been used frequently throughout this paper. In this context ‘access’ and ‘use’ mean different things. A person who receives and watches a broadcast is just accessing the service. Merely watching a subscription broadcast (even without having paid the subscription fee) does not breach the broadcaster’s copyright in the broadcast or any copyright in the underlying content of the broadcast. If the recipient copies the broadcast (eg by using a video recorder) or distributes it on to other persons online or by cable, they are doing more than just accessing it – they are also using it. Doing more than just accessing the broadcast service is likely to involve a breach of the copyright in the broadcast and, possibly the content of the broadcast.

9. The subscription broadcast industry has made many representations to the Government advocating for the criminalisation of all forms of unauthorised access to and use of subscription broadcasts. The industry has informed the Government that there are many persons accessing subscription broadcast services through unauthorised means and without payment for the service being received. Referred to by the industry as ‘subscription broadcast piracy’ or ‘pay TV piracy’, the industry considers the activity to be theft of the service it provides. The industry also considers that criminalising all forms of unauthorised access to and use of subscription broadcast services would have a deterrent effect and reduce the incidence of the unauthorised activity.

10. In response to the concerns of the subscription broadcast industry, the Government has undertaken to review its policy not to criminalise the private or domestic use of a broadcast decoding device to access a subscription broadcast and, at the same time, to consider other concerns of the industry in relation to unauthorised access to and use of subscription broadcasts.⁵

⁵ Some submissions from the industry have pointed to deficiencies in the definition of ‘broadcast decoding device’ in the Copyright Act. This paper does not deal with this issue. The form of any amendments that may arise from this policy review (including any amendments to existing provisions) will be considered once the underlying policy is settled.

11. In correspondence with the United States Trade Representative in November 2004 concerning the commencement of the AUSFTA, the Government indicated as follows:

As a result of approaches from Australian stakeholders, the Government will shortly undertake, as a separate exercise, a review of our domestic policy relating to criminalisation of all forms of satellite signal piracy, including unauthorised distribution or receipt of signals by commercial establishments and within the home, that will conclude no later than 1 July 2005.⁶

⁶ Letter from the Minister for Trade, the Hon Mark Vaile MP, to the United States Trade Representative, Robert B Zoellick. November 2004: http://www.dfat.gov.au/trade/negotiations/us_fta/final-text/letters/ip_vaile_zoellick.pdf. While the undertaking referred specifically to 'satellite signal piracy', the relevant provisions of the Copyright Act considered as part of this review apply to encoded broadcasts whether transmitted by satellite or cable.

2. The subscription broadcast industry, services and concerns

The subscription broadcast industry

12. This section provides background information on the subscription broadcast industry, including the various bodies involved in the industry and the services provided by the industry. It also outlines the industry's concerns over unauthorised access to and use of subscription broadcasts and some of the impacts of unauthorised activities on the industry.

13. The subscription broadcast industry includes:

- major pay TV platforms or providers including FOXTEL, AUSTAR and OPTUS Television and some smaller carriers such as Neighbourhood Cable, TARBS and TransACT that deliver subscription broadcasting and bundled services to particular markets (referred to as 'subscription broadcast providers' or 'providers' in this paper), and
- bodies that provide channels and programs for the providers to distribute to subscribers⁷ and, in some cases, also produce a subscription TV channel for direct distribution to their own commercial subscribers (called 'channel providers' in this paper).⁸

14. In addition to the above there are many persons whose livelihood is connected, in one way or another, with the subscription broadcast industry. These include the employees of the subscription broadcast providers, related support industries and channel providers, actors, scriptwriters, camera operators and the many others involved with the making and broadcasting of program material.

Services provided by the subscription broadcast industry

15. According to the Australian Subscription Television and Radio Association (ASTRA), the services provided by the industry can be loosely divided into two types:

⁷ Examples of channel providers are Sky Channel Pty Limited (Sky Channel) and Premier Media group Pty Limited (Premier), Discovery Channel, Disney Channel, Cartoon Network and Nickelodeon. The Australian Subscription Television and Radio Association lists 44 channel providers as members.

⁸ For example, Sky Channel and Premier.

- commercial subscription services – offered by both the subscription broadcast providers and some channel providers to commercial premises (eg hotels or clubs) for screening to the general public, and
- residential subscription services – offered only by the subscription broadcast providers and only for domestic/residential use, subject to an express condition that they not be displayed in public.

16. In some cases, an industry member is both a subscription broadcast provider and a channel provider. For example, as a subscription broadcast provider Sky Channel Pty Limited provides the Sky Channel Commercial Service which is broadcast via satellite to hotels, clubs, TAB outlets and other applicable businesses. As a channel provider, it provides the Sky Racing Channel, which is a packaged channel provided to other subscription broadcast providers for broadcasting by them to relevant domestic subscription broadcast service customers. Subscribers to Sky Channel Commercial Service pay more for a channel for viewing in public and licensed areas than a domestic subscriber who subscribes to a service that includes Sky Racing Channel.⁹

17. A contractual relationship exists between a subscription broadcast provider and a subscriber and the contract determines the terms of supply for the service being provided. According to subscription broadcast industry representations, the terms of supply of the domestic subscription TV services include:

- specific prohibition of the resupply, splitting or redistribution of the service
- specific prohibition of the supply of the service to any location other than the subscriber's private residence
- specific prohibition of the use of the service in any public viewing area, and
- authority to use the reception equipment supplied to access the encoded broadcast only in accordance with the terms and conditions of supply for private residential and non-commercial use at the subscriber's nominated address.

⁹ The subscription fee for the Sky Channel Commercial Service varies from venue to venue. It is based on an industry related fee scale that takes into account the size and volume of trading activity for the relevant venue. [<http://www.skychannel.com.au/subscribers/>]

18. A subscriber gains access to the subscription broadcast service through a combination of equipment. In the case of a cable broadcast service, the subscription broadcast provider will organise for the subscriber's premises to be cabled by the provider. A set-top box (and, for many services a smart card) will be supplied by the provider. In the case of a satellite broadcast service the subscription broadcast provider will supply and install a satellite dish, cabling, a set-top box and a smart card that is programmed to decode the encoded broadcast so that the subscriber can access the channels included in their subscription.¹⁰

Unauthorised access to and use of a subscription broadcast

19. Unauthorised access to and use of a subscription broadcast service can be achieved by various means and can be carried out by persons who are subscribers to a subscription broadcast service as well as non-subscribers. Such acts are briefly outlined below.

20. Many acts of unauthorised access to and use of subscription broadcasts are already addressed though the civil remedies and criminal offences in the Copyright Act. A summary of the current criminal offences and civil remedies in the Copyright Act concerning subscription broadcasts is set out in Appendix 2 of this paper.

21. Unauthorised access is primarily achieved through the use of unauthorised equipment. For example, a non-subscriber may need a satellite dish, cabling, set top box and a fraudulent smart card to access a subscription broadcast service. Sometimes all this equipment will be acquired, installed and used without any authorisation by a subscription broadcast provider. In other cases, such as where the premises may already have the necessary cabling and satellite dish due to a previous resident having been a subscriber, only the set top box and fraudulent smart card may be needed for unauthorised access. According to the subscription broadcast industry, subscribers to a service have also been known to gain unauthorised access by the use

¹⁰ The equipment supplied to a subscriber and used to access the service generally remains the property of the subscription broadcast provider. For example, in the case of a FOXTEL service this includes the set-top unit, the personal digital recorder, the remote control unit, smart card, a DIGIPATH, the cabling from the wall-plate to the set-top unit, and from that unit to the subscriber's television as well as any other equipment already installed at the subscriber's address. Certain infrastructure and approvals may need to be in place concerning provision of a subscription broadcast service to units and townhouses. See <http://www.foxtel.com.au/176.htm>.

of a fraudulent smart card which enables the subscriber to access more channels than they have paid for in their subscription.

22. In 2003-2004, FOXTEL and AUSTAR introduced new technology for accessing its satellite pay TV services that was aimed at eliminating unauthorised accessing of their services.¹¹ The key element of the initiative was the introduction of more secure smart cards used to access the services. Persons using a fraudulent smart card to access the services were effectively cut-off from receiving the signal. FOXTEL has stated publicly that during this upgrade 10-15 percent of users were identified as receiving the service via unauthorised smart cards. While noting that the technology upgrade had 'substantially reduced' the problem FOXTEL also stated that 'there are always going to be people working on the fringes, trying to crack our encryption technology'.¹²

23. Of increasing concern to the subscription broadcasting industry is a relatively new form of unauthorised activity involving encoded broadcasts called 'card-sharing'. Card sharing involves the use of satellite dishes, set top boxes and computers in multiple locations networked through the Internet. It involves the use of a legitimate smart card that is made accessible to a network of 'clients' via the Internet. Clients on the network are able to access the encryption decoding key from the legitimate smart card enabling the client to access an encoded broadcast through their own satellite dish and set top box.

24. The person setting up the network with the legitimate smart card may be a subscriber who has made their card available on-line (in breach of their subscriber agreement) so that others can access the decrypting key. Alternatively, the person may be a non-subscriber who has obtained a legitimate smart card by some means (such as theft) and made it available on-line to clients on the network. Regardless of whether the person setting up the network is a subscriber or not, card sharing potentially enables many persons to access a subscription broadcast service without a subscription.

¹¹ FOXTEL Press releases 'Satellite TV Piracy to be wiped out' [4 November 2003] and 'FOXTEL targets piracy' [2 December 2003].

¹² *Herald Sun*, 3 March 2005, 'Pay-TV's pirates under fire', 43 (quoting FOXTEL's Director of Corporate Affairs, Mark Furness).

25. As it is an offence to make a broadcast decoding device available online, the person who has set up a card-sharing network and made the smart card available online is likely to be committing an offence.¹³ Civil remedies are also available against that person.¹⁴ However, the ‘client’ of that person is only committing an offence if the broadcast is used ‘by way of trade or with the intention of obtaining a commercial advantage or profit’.¹⁵ It is not an offence under Commonwealth law if a subscription broadcast is accessed without authorisation for purely private and domestic viewing. However, civil remedies may be available against the unauthorised recipient.¹⁶

26. The subscription broadcast industry also has concerns about other unauthorised activities involving subscription broadcast services that the industry considers are not adequately dealt with under Commonwealth law. These largely concern unauthorised uses by persons who have subscribed to a subscription broadcast service and following decoding, breach their agreement with the subscription broadcast provider by using the service in an unauthorised manner. Unauthorised uses by subscribers include activities such as service distribution, relocation and signal splitting.

27. Service relocation occurs when a subscriber moves the TV with the set-top box and smart card supplied by the subscription broadcast provider to another location without the provider’s authorisation. For example, a subscriber may relocate a domestic subscription service authorised for private residential use into a commercial public viewing area (possibly licensed premises) to avoid paying the higher commercial subscription rate.

28. Signal splitting occurs when unauthorised cabling is used to distribute the decoded broadcast to other parts of the same premises or to other premises. For example, a hotel owner who has legitimately subscribed to a residential service may

¹³ Section 135AS(1)(f) and possibly, section 135AS(1A) (if done by way of trade or with the intention of obtaining a commercial advantage or profit) of the Copyright Act. Arguably, a legitimate decoding device would become a ‘broadcast decoding device’ as that term is defined in section 135AL because by having been made available online it has been ‘adapted to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster’.

¹⁴ Section 135AN(1)(b)(vi), Copyright Act.

¹⁵ Section 135AS, Copyright Act.

¹⁶ Sections 135ANA(1) and (1B), Copyright Act.

split the signal output of a set-top box so that it can be viewed in both the residential part of the premises and an adjoining commercial public viewing area connected via a separate (unauthorised) cable. Alternatively, the signal could be split so that it can be viewed simultaneously in more than one premises. These activities are discussed in greater detail later in the paper.

Impacts of unauthorised activities

29. The Government acknowledges that unauthorised activities concerning subscription broadcasts can affect legitimate business interests of subscription broadcast providers and inhibit the growth of subscription broadcast services in Australia. Unauthorised access to, and use of, subscription broadcast services cause direct loss of revenue to both subscription broadcast providers and channel providers. Where no subscription fee (or a lesser subscription fee) is paid for the broadcast accessed, both the subscription broadcast provider and relevant channel providers are not receiving the appropriate fees for the services accessed. As subscription broadcast providers pay channel providers for the channels included in a subscription service, channel providers also suffer reduced incomes if the appropriate subscription fees have not been paid for the service.

30. In some cases, the loss may be significant in financial terms. For example, a hotel might access Sky Racing through a domestic subscription service supplied through FOXTEL or AUSTAR and use it in a public-viewing area instead of subscribing to the Sky Channel commercial service which is the appropriate service for the use being made of the encoded broadcast. In this case the provider would still receive a subscription fee for the domestic subscription. Sky Channel would be paid by the provider for supply of the Sky Racing channel but is effectively deprived of the more appropriate commercial service subscription fee.

31. The more people who are accessing a subscription broadcast service without paying the appropriate subscription fee, the less revenue the industry has to invest in the service provided, including program development. Therefore, unauthorised access may have an indirect impact on the many persons whose livelihood is connected in one way or another with the subscription broadcast industry. In addition, legitimate

subscribers may possibly be paying more for the service because there are those who access it without paying for it.

32. To fully assess the impact of the unauthorised activities that are not currently criminal offences, it would be necessary to know the prevalence of unauthorised access and use. As most of these activities are conducted within private premises they are difficult to detect and, therefore, the prevalence of the activity is difficult to assess. As a consequence, it is difficult to estimate the loss of income to the subscription broadcast industry arising from all forms of unauthorised access to and use of subscription broadcasts. In years past the industry has estimated from evidence of such activities that there are significant amounts of potential lost revenue.¹⁷

33. With the introduction of improved services such as the new digital television service and better encryption technology to protect that service it would be expected that the incidence of unauthorised access has decreased. In addition, media reporting of successful court action against those who engage in the authorised activities may have had a deterrent effect over time.¹⁸ At the same time new forms of unauthorised access, such as card-sharing, have emerged. It is not known whether such activity is confined to a relatively small number of technology savvy users or whether it is widespread. For all these reasons, the extent to which past industry estimates of potential lost revenue remain relevant today is not known.

Emerging technology affecting subscription broadcasts

34. This paper has not dealt with any particular issues concerning unauthorised access and use of subscription broadcasts that might arise with emerging technology. For example, increasingly compressed formats, wireless technology and the use of electricity cables to distribute subscription-based services may create new opportunities for unauthorised activities. To the extent that new and emerging technologies raise different issues to those discussed in this paper, submissions on these issues are welcome.

¹⁷ It has been reported that prior to the introduction of the 2003-04 technology upgrade FOXTEL was losing \$50 million a year due to signal piracy: 'Pay-TV's pirates under fire', *Herald Sun*, 3 March 2005, 43.

¹⁸ For example, a number of court actions by Sky Channel against hotels pirating its racing service in 2003 may have reduced the incidence of this form of unauthorised activity: Tab Limited media report of 26 February 2003, 'Sky Pirates Pay The Price'. Further media releases concerning enforcement actions are available at <http://www.astra.org.au/news.asp?section=2&option=4&content=3&type=2>.

3. Relevant criminal law and policy

35. This section provides general information about relevant criminal law and background material on Commonwealth criminal law policy.

When is conduct criminal in nature?

36. An examination of criminal law was conducted by the Australian Law Reform Commission (ALRC) in its *Principled Regulation* report. The ALRC stated:

The main purposes of criminal law are traditionally considered to be deterrence and punishment. Central to the concept of criminality are the notion of individual culpability and the criminal intention for one's actions. ... Traditional criminal offences and non-criminal contraventions can in many respects be distinguished by the inherent nature of the actions themselves. A key characteristic of a crime, as opposed to other forms of prohibited behaviour, is the repugnance attached to the act, which invokes social censure and shame. This is clearly the case in relation to 'traditional' criminal offences such as those involving violence or violation of another's property or person.¹⁹

37. The Commonwealth's Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers (the Criminal Law Guide), states:

Certain conduct should be almost invariably classified as criminal due to the degree of malfeasance or the nature of the wrongdoing involved. For example, conduct that results in physical or psychological harm to other people (murder, rape, terrorist acts) or conduct involving dishonest or fraudulent conduct (false or misleading statements, bribery, forgery). In addition, criminal offences should be used where the relevant conduct involves considerable harm to society, the environment or Australia's national interests, including security interests.²⁰

38. The Criminal Law Guide also states that a range of factors must be considered in determining when the criminal law should apply. These include:

¹⁹ ALRC, Report 95, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, December 2002, 2.9 and 2.10.

²⁰ Australian Government [Issued by authority of the Minister for Justice and Customs], *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*, February 2004, 4.1 (Criminal Law Guide).

- What is the nature of the conduct sought to be deterred?
- Does the conduct seriously harm other people?
- Does the conduct in some way so seriously contravene our fundamental values as to be harmful to society?
- Is it appropriate to use criminal enforcement powers in investigating the conduct?
- Is the criminal law appropriate for dealing with the undesirable conduct in question?
- How is similar conduct regulated in the proposed legislative scheme and other Commonwealth legislation?²¹

39. When Parliament enacts legislation creating an offence it is effectively saying that this activity seriously contravenes the fundamental values of our society and that it is appropriate to use public monies and criminal enforcement powers in investigating and prosecuting those who engage in such conduct.

Model Criminal Code Committee examination of theft and fraud offences

40. In 1995 a detailed examination of theft, fraud, bribery and related offences was conducted by the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (the Committee) for the purposes of the development of a Model Criminal Code in Australia (the Model Criminal Code Chapter 3 Report).²²

Under the Australian Constitution the Commonwealth has limited constitutional power to enact laws. While the Commonwealth has enacted specific criminal law legislation²³ and criminal offence provisions in specific Commonwealth legislation,

²¹ Criminal Law Guide, above n 25, 4.1.

²² Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Model Criminal Code Chapter 3 Theft, Fraud, Bribery and Related Offences*, Final Report, December 1995 (Model Criminal Code Chapter 3 Report).

²³ The *Crimes Act 1914* and the *Criminal Code Act 1995*.

general theft and fraud offences regarding private property are contained in State and Territory Criminal Codes or Crimes Acts. The Model Criminal Code project was aimed at the development of uniform criminal codes for Australian jurisdictions.

41. While the particular way in which each jurisdiction deals with theft or fraud in their respective criminal legislation may differ, it is worth considering what the Committee said in relation to theft and fraud offences.

The report articulated six elements of *theft* as follows:

- (1) dishonesty
- (2) appropriation
- (3) property
- (4) belonging to another
- (5) intention to deprive permanently, and
- (6) the requirement that all the elements exist at the same time.²⁴

42. Many copyright owners consider that activity concerning infringing copyright material is theft.²⁵ While statute law has extended the scope of theft offences to intangible things it has not gone as far as regarding breach of copyright as theft. The Model Criminal Code Chapter 3 Report noted as follows:

Mere breach of copyright or use of a trade secret might involve a breach of copyright or use of the trade secret but would not be theft ... because there is no intent to permanently deprive the owner.²⁶

43. The report supported inclusion of separate fraud offences in the Model Criminal Code for obtaining property by deception and obtaining a financial advantage by deception. The offence of obtaining property by deception (with the various elements underlined) was defined as follows:

²⁴ Model Criminal Code Chapter 3 Report, above n 26, 31.

²⁵ See for example, the Australian Federation Against Copyright Theft (AFACT) www.afact.com.au/.

²⁶ Model Criminal Code Chapter 3 Report, above n 26, 47.

A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, is guilty of an offence.²⁷

44. The offence of obtaining a financial advantage by deception (with the various elements underlined) was defined as follows:

A person who by any deception dishonestly obtains for himself, herself or another any financial advantage is guilty of an offence.²⁸

45. The Committee did not define ‘financial advantage’ and the report noted that how far the concept extended was ‘open to question but what is obtained must be characterisable somehow as an advantage in money terms’.²⁹

46. In relation to the relevant offences in the Model Criminal Code Chapter 3 Report, ‘dishonest’ was stated to mean ‘dishonest according to the standards of ordinary people and known by the defendant to be dishonest according to the standards of ordinary people’.³⁰ The report also stated that in a prosecution for an offence, dishonesty is a matter for the trier of fact. While dishonesty was an element of the theft and fraud offences, the Committee recommended against the Model Criminal Code containing a general dishonesty offence.³¹

Theft and fraud offences in State and Territory legislation

47. Given that the issue of concern is the accessing of services provided by privately owned businesses, some may consider that if the law is to provide a remedy, or if the issue of accessing and using the service without paying for it should be an offence, then it is a matter that should be dealt with under State and Territory law. It is therefore relevant to examine what State and Territory law may be applicable.

²⁷ Model Criminal Code Chapter 3 Report, above n 26, 136.

²⁸ Model Criminal Code Chapter 3 Report, above n 26, 146.

²⁹ Model Criminal Code Chapter 3 Report, above n 26, 147.

³⁰ Model Criminal Code Chapter 3 Report, above n 26, 32, 140.

³¹ Model Criminal Code Chapter 3 Report, above n 26, 153 – 171.

48. All State and Territory jurisdictions have enacted comprehensive legislation criminalising theft, deception and like offences. These offences are generally contained in a specific part relating to property offences in the Criminal Code (or equivalent) of each State or Territory.

Theft offences

49. Theft is generally defined as ‘dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it’.³² The alternative offence of stealing is defined as ‘[a] person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person any property’.³³ Despite slight variations in each definition all offences are likely to be dealt with similarly in each different State or Territory. The offences rely on some degree of fraudulence or dishonesty as an element of the offence. While there is no clear definition of what would constitute a fraudulent or dishonest action, examples of exceptions to these definitions are often contained in the legislation.³⁴

50. Theft, stealing or larceny offences depend further on the notion of ‘property’ being taken. Property, in most States and Territories, is defined as money and all other property real or personal including things in action and other intangible property.³⁵ Some States and Territories have enacted more complex definitions of ‘property’³⁶ while others have left the term undefined.

51. Receiving stolen property is often a more serious offence than stealing itself. The offence of receiving is committed ‘if the person dishonestly receives stolen

³² Section 308, *Criminal Code* 2002 (ACT).

³³ Section 371, *Criminal Code* (WA).

³⁴ For example, see section 303, *Criminal Code* 2002 (ACT) which exempts from the definition of dishonest the situation where a person appropriates the property in the belief that the person to whom the property belongs cannot be discovered by taking reasonable steps.

³⁵ Section 71(1), *Crimes Act* 1958 (Vic).

³⁶ For example, see section 371(7) of the *Criminal Code* (WA) which defines property as ‘any description of real and personal property, money, debts, bank credits, and legacies and all deeds and instruments relating to or evidencing the title or right to any property or giving a right to recover or receive any money or goods and also includes not only such property as has been originally in the possession or in the control of any person but also any property in which or for which it has been converted or exchanged and anything acquired by the conversion or exchange, whether immediately or otherwise’.

property, knowing or believing the property to be stolen'.³⁷ Some jurisdictions have included this offence in the same category as stealing, while others have dealt with it as an offence akin to fraud.

52. The subscription broadcast industry regards the unauthorised access to and use of a subscription broadcast as 'theft' and akin to offences such as theft of electricity or gas which is a specific offence in some State and Territory jurisdictions³⁸ and covered by more general theft offences in others. While it is acknowledged that such offences clearly involve obtaining a benefit/service without paying for it, the historical context of these offences is relevant. It is likely that in those jurisdictions where there is a specific theft offence in relation to gas or electricity, those offences were enacted at a time when the state was the owner and sole provider of those services. Thus criminalising this activity was effectively protecting public resources and public revenue. It is only with the subsequent privatisation of these services that they now cover services provided by private sector bodies.

Fraud offences

53. State and Territory legislation differs considerably in its approach to deception and dishonesty offences. These types of fraud offences are often worded broadly with some States or Territories including additional narrower provisions. Deception, as an offence, is committed when a person dishonestly benefits him/herself or a third person, or dishonestly causes a detriment to the person subjected to the deception or a third person.³⁹ New South Wales and Victoria have specifically included in their definition of deception 'an act or omission done to a machine that is designed to operate by means of payment or identification to make a response that the person doing or omitting to do the act is not authorised to cause the machine to make'.⁴⁰ South Australia has preferred to enact a specific provision on the dishonest manipulation of machines.⁴¹

³⁷ Section 313, *Criminal Code 2002* (ACT).

³⁸ See, for example, section 64 of the *Electricity Supply Act 1995* (NSW) and section 65 of the *Gas Supply Act 1996* (NSW).

³⁹ Section 139, *Criminal Law Consolidation Act 1935* (SA).

⁴⁰ Section 178BA, *Crimes Act 1900* (NSW) and section 81, *Crimes Act 1958* (Vic).

⁴¹ Section 141, *Criminal Law Consolidation Act 1935* (SA) which states that 'a person who dishonestly manipulates a machine in order to benefit him/herself or another, or cause a detriment to another is guilty of an offence.

54. Queensland and Western Australia allow a broader range of offences to be categorised as fraud under the application of the provision ‘Acts done with intent to defraud’.⁴² Under this provision, ‘[w]hen an act which causes injury to property, and which would be otherwise lawful, is done with intent to defraud any person, it is unlawful’.

Applicability of State and Territory offences

55. It is possible that the act of receiving a subscription-based service without paying for that service may already be covered by an existing theft or fraud offence under State or Territory legislation. However, considerable variation exists between the offences across the different jurisdictions. In some jurisdictions with broad definitions of property and offences for conversion of property, unauthorised access and use of a subscription broadcast may be covered under their stealing or theft offences. In other jurisdictions it may fall under the offence of dishonestly obtaining a financial advantage. Therefore, it is not clear whether this activity would be a criminal offence in all jurisdictions. In addition, there would be considerable differences in the prosecutions across the various jurisdictions due to the variations in the elements of the respective offences.

Theft and fraud offences in Commonwealth legislation

56. Because of its constitutional limitations, for the Commonwealth to criminalise an activity there must be an appropriate Commonwealth connection. The Commonwealth *Criminal Code 1995* (Commonwealth Criminal Code) currently contains theft and fraud offences. However, these offences only apply to theft or destruction of Commonwealth property and defrauding the Commonwealth.

57. The Commonwealth Criminal Code also contains telecommunications offences.⁴³ A dishonesty offence in relation to telecommunications services was originally inserted into the Crimes Act when the Commonwealth was the provider of all telecommunications services in Australia.⁴⁴ With the subsequent changes to the

⁴² Section 459, *Criminal Code 1899* (Qld) and section 442, *Criminal Code* (WA).

⁴³ The telecommunications offences are in Division 474 and are part of Chapter 10 concerning the National Infrastructure.

⁴⁴ It was inserted as section 85ZF of the *Crimes Act 1914* in 1989.

way telecommunications services are provided in Australia the offence now covers activities in relation to services provided by private sector bodies.

58. The general dishonesty offences with respect to a ‘carriage service provider’ are currently found in section 474.2 which states as follows:

Obtaining a gain

(1) A person is guilty of an offence if the person does anything with the intention of dishonestly obtaining a gain from a carriage service provider by way of the supply of a carriage service.

Causing a loss

(2) A person is guilty of an offence if the person does anything with the intention of dishonestly causing a loss to a carriage service provider in connection with the supply of a carriage service.

(3) A person is guilty of an offence if:

- (a) the person dishonestly causes a loss, or dishonestly causes a risk of loss, to a carriage service provider in connection with the supply of a carriage service; and
- (b) the person knows or believes that the loss will occur or that there is a substantial risk of the loss occurring.⁴⁵

59. Consistent with the manner in which ‘dishonesty’ was defined for the purposes of the Model Criminal Code, the test for ‘dishonesty’ for the purposes of the above offences is ‘according to the standards of ordinary people and known by the defendant to be dishonest according to [those] standards’.⁴⁶ As in the Copyright Act, carriage service provider is defined in the Criminal Code by reference to the *Telecommunications Act 1997*. This definition does not include broadcasters.⁴⁷

Effect of a criminal conviction

60. Criminal offences are not enacted lightly as a conviction for a criminal offence has serious consequences for the convicted person. The Criminal Law Guide states that the effect of a criminal conviction is perhaps the most important factor to be

⁴⁵ The current maximum penalty for these offences is imprisonment for 5 years.

⁴⁶ Section 474.1, Commonwealth Criminal Code.

⁴⁷ Section 93, *Telecommunications Act 1997*.

considered in deciding whether a provision should be civil or criminal. The following extract from the Criminal Law Guide sets out these consequences.

Conviction of a crime carries with it a range of consequences beyond the immediate penalty - whether this is imprisonment or a pecuniary penalty:

A person who is convicted of certain offences will be ineligible to hold public office and may be removed from a position they already hold. For example a person who has been convicted of an offence punishable by imprisonment for 12 months or longer cannot become a Senator or member of the House of Representatives, *Commonwealth Constitution* section 44(ii).

Subject to the spent conviction provisions in Part VIIC of the *Crimes Act 1914*, a person may be required to disclose the fact of their criminal conviction in a range of circumstances. For example, when seeking employment to care for minors or work in a law enforcement agency.

The person may be ineligible to travel to many countries.

A conviction may affect also the right of a non-citizen to remain in Australia under the *Migration Act 1958*.

A person, whether a natural person or a body corporate, may be disqualified from becoming accredited under various legislation, for example under section 57 of the *Employment Services Act 1994*.

A person may be ineligible to be a director, principal officer or auditor of a company, see for example section 245 of the *Life Insurance Act 1995*.

In addition, a criminal conviction carries with it a social stigma, particularly where the conviction is accompanied by imprisonment. As with the other consequences discussed above, this will have more impact on a natural person than on a body corporate. This is an important factor in determining comparative civil and criminal penalties, and is a strong justification for lower criminal penalties for individuals.

Imprisonment is only available as a penalty for the commission of a criminal offence by a natural person. It is the most onerous penalty that can be imposed on an individual.⁴⁸

⁴⁸ Criminal Law Guide, above n 25, 4.1.

4. Unauthorised access and use not covered by the Copyright Act and the issue of criminalisation

61. If the Commonwealth were to criminalise any further activities concerning subscription broadcasts, it must be clear about exactly what behaviour is to constitute an offence. Distinguishing the activities that are to be covered from those that are not is an important part of the policy development process. It assists in identifying what are to be the elements of any offence provisions that may result.

62. This section examines specific unauthorised activities involving subscription broadcasts not currently criminalised under the Copyright Act and considers factors for and against criminalisation of such activity by the Commonwealth. As the primary focus for this policy review is whether the Government should change its current policy of not criminalising unauthorised access and use of subscription broadcasts in a purely private and domestic context, this activity is discussed first. The section then deals with other unauthorised activities in relation to subscription broadcasts of concern to the subscription broadcast industry.

Unauthorised access to and use of a subscription broadcast in the home

63. Unauthorised access to and use of a subscription broadcast in a purely domestic context may occur in several ways. It would cover each of the following situations:

- a person uses a broadcast decoding device to access a subscription broadcast⁴⁹
- a person receives a subscription broadcast that has been decoded and distributed by another person, or
- a subscriber to a domestic service uses a broadcast decoding device to access more channels than they have paid for in their subscription.

Breach of contract?

64. If a subscriber uses a broadcast decoding device to access more channels than they have paid for in their subscription, the subscription broadcast provider should have a remedy for breach of contract against the subscriber. However, with the

⁴⁹ This would include a card-sharing 'client'.

introduction of the new version of the smart card in 2004 it is likely that most cases of unauthorised access would be carried out by non-subscribers where there is no contract and no contractual remedy available to the provider.

A breach of copyright?

65. It is important to note that merely accessing (or watching) a subscription broadcast does not breach any copyright in the broadcast or the underlying content of the broadcast. An infringement of the copyright of both the broadcast and the underlying content would occur if, for example, the broadcast was copied without (express or implied) permission. In this case the usual remedies for breach of copyright would apply. This is likely to be the case with increasing use of digital video recorders.

66. Digital video recorders constantly record the broadcast to enable the pause and replay functions to operate. This represents a major shift from video cassette recorders where it is generally only particular programs that are recorded. As the use of digital video recorders increases, including by persons who have accessed a subscription broadcast service without authorisation, there will be a corresponding increase in the copying of broadcasts and the content of broadcasts. It has been argued that an authorised subscriber issued with a digital video recorder as part of their subscription may have an implied licence from the broadcaster to record the broadcast.⁵⁰ However, an unauthorised recipient would not and this would constitute a breach of the reproduction right in the broadcast and the underlying content of the broadcast. Copyright owners would be entitled to take civil action against the unauthorised users for any breaches of their copyright and the usual offences in the Copyright Act relating to infringing material would apply.

⁵⁰ The existence or extent of any implied licence is unclear. The extent to which a broadcaster could give an implied licence in relation to the reproduction of the underlying content of the broadcast is even more unclear. This raises issues regarding use of copyright material and whether any of the 'fair dealing' exceptions apply. The Department has recently released an issues paper on options for including new exceptions to the Copyright Act based on principles of 'fair use'. The issues paper is available at: www.ag.gov.au.

Existing policy concerning criminalising unauthorised access

67. As has already been stated, while copyright subsists in a broadcast, accessing a subscription broadcast without paying for it does not breach any copyright in the broadcast or its underlying content. While the offences concerning broadcast decoding devices are contained in the Copyright Act they are not directed at punishing copyright infringing activity. These offences proscribe more serious acts that provide the means for **accessing** subscription broadcasts without authorisation, particularly where there is some intention of gaining commercial advantage or profit from the use of that broadcast.

68. The public policy basis for criminalising activity involving acts concerning unauthorised access and use of subscription broadcasts is clearer when some commercial advantage or profit is involved. The offender is not just receiving the service for their personal enjoyment alone. The person is deliberately engaging in some use of the broadcast received for some commercial advantage or profit. The public policy basis for criminalising unauthorised access is less clear when the only use made of that broadcast is to view it in the privacy of one's own home.

69. In contrast to other countries' copyright laws, Australia's Copyright Act reflects the policy that personal use of a broadcast decoding device enabling unauthorised access to a subscription broadcast for purely private and domestic use should not be criminalised. Criminal law enforcement against an individual for using a broadcast decoding device in their home is an intrusion into the private sphere.

Factors to be considered in determining whether the criminal law should apply

70. The previous section of this paper listed factors that should be considered in determining whether behaviour should be subject to the criminal law.⁵¹ The unauthorised activities listed in paragraph 62 above must be assessed against these and other relevant factors.

71. The **first factor is the nature of the conduct sought to be deterred**. The above examples of unauthorised access involve obtaining a subscription broadcast

⁵¹ See paragraph 37.

service without paying for it (or without paying the correct subscription fee). The end result of obtaining that service is that the recipient is able to access copyright material that the various copyright owners have determined should be communicated to the public by way of a subscription-based service.

72. One issue is whether this activity is essentially the same as obtaining the benefit of any other fee-based service without paying for it (eg by some fraudulent means). In terms of the nature of the activity there is clearly an element of dishonesty.

73. However, dishonesty alone is not enough to warrant criminalising an activity. Not all dishonest acts are criminal offences. In most cases, dishonesty is only one element of the offence. The question remains whether this particular dishonest activity is of such a nature that it ought to be criminalised.

74. The **second factor is whether the conduct seriously harms other people**. The conduct clearly results in no physical harm to others. Any harm that does result to others is commercial in nature. While it does not necessarily follow that every person who dishonestly accesses the service is a potential legitimate subscriber, the conduct results in loss of potential income to the subscription broadcast industry. It may also have flow-on commercial ‘harm’ to legitimate subscribers who arguably have to pay more for the service than they may have to if all persons accessing the service were paying for it.

75. That said, an individual can only be held accountable under the law for their own acts and the loss that arises from those acts. In the case of a person who has accessed a subscription broadcast, the commercial loss to the subscription broadcast provider is the amount of the subscription for the particular service that has been accessed.⁵²

76. The **third factor is whether the conduct in some way so seriously contravenes our fundamental values as to be harmful to society**. It has already been established in answer to the first factor that the nature of the activity is dishonest.

⁵² For example, the subscription pricing for FOXTEL’s Platinum Package is currently \$97.95 per month which includes the following FOXTEL services: Digital Basic, Three Entertainment tiers and Movies De Luxe packages, two FOXTEL Box office Movies and FOXTEL Digital magazine [FOXTEL Pricing Summary as at February 2005: http://foxtel.com.au/digital_terms.htm].

As 'dishonest' means dishonest 'according to the standards of ordinary people' some examination of the activity is useful to determine whether it meets this test.

77. The community is aware that 'pay TV' is a subscription-based service requiring payment of a fee to receive the service. The equipment used to access a subscription broadcast service is designed for the specific purpose and, in cases of authorised access, is supplied by the subscription broadcast provider. In most cases of unauthorised receipt of a subscription broadcast service the recipient would have taken an active role in order to receive the broadcast. This may include buying a fraudulent smart card, setting up the necessary satellite dish, set-top box or downloading software from the Internet to participate in a card-sharing network. To receive a subscription broadcast without any subscription there must clearly have been deliberate action taken to receive a service that has a fee attached without payment of that fee.

78. It is likely that the activity described above would be considered to be dishonest according to the standards of many ordinary people. The question for this review is whether the behaviour so seriously contravenes our fundamental values that it ought to be made a criminal offence - to punish those who engage in it and deter those (and others) from engaging in that behaviour again.

79. The **fourth factor is whether it is appropriate to use criminal enforcement powers in investigating the conduct.** Once conduct is criminalised there are powers to enforce that law. Those powers allow the police to use a full range of coercive law enforcement powers such as entry, search and seizure which they would otherwise not be able to use. The use of criminal enforcement powers to investigate criminal conduct is a commitment of public money and resources.

80. If the conduct that is the subject of this review is viewed as conduct deliberately undertaken to avoid payment of a fee for a subscription service, or the appropriate subscription fee for the service being accessed, then the use of criminal enforcement powers may be considered to be appropriate. However, account must be taken of the fact that in most cases, what is in issue is activity being conducted in private premises. People have an expectation that the security of their residence and their privacy will be respected. Most consider that private (non-commercial) activity carried out in the

privacy of their own home that does not hurt anyone is their business. Governments are understandably reluctant to allow police to enter private homes unless there are very good reasons to do so.

81. The Senate Standing Committee for the Scrutiny of Bills examined entry and search provisions in Commonwealth legislation in 1999-2000. In the Executive Summary to the Committee's report the Committee set out principles governing the grant of powers of entry and search by Parliament. The Committee stated, among other things that intrusion into private premises 'is warranted only in specific circumstances where the public interest is objectively served'.⁵³

82. If an activity is criminalised then there is an expectation that the criminal law will be enforced. Strong public policy grounds must exist before activity carried out in a purely private or domestic context is criminalised.

83. The **fifth factor is whether the criminal law is appropriate for dealing with the undesirable conduct in question.** This involves similar considerations to the issues above.

84. One reason for making personal use of a broadcast decoding device (and other forms of unauthorised access) an offence may be the deterrent value of the behaviour clearly being classified as criminal. However, deterring undesirable conduct is just one factor for consideration by governments in deciding whether a particular activity ought to be criminalised. It is noted that the Commonwealth has ensured that civil remedies are available under the Copyright Act to assist subscription broadcast providers and channel providers in relation to unauthorised receipt of subscription broadcasts.⁵⁴ The availability of a civil remedy alone may prove to be sufficient deterrent to people accessing subscription broadcasts without authorisation.

85. While there is behaviour that may be clearly undesirable from a societal perspective, as discussed in the previous section, a criminal conviction carries with it a range of consequences beyond the immediate penalty for the crime. These include

⁵³ Parliament of Australia, Senate Standing Committee for the Scrutiny of Bills, *Fourth Report of 2000: Entry and Search provisions in Commonwealth Legislation*, 6 April 2000, 49.

⁵⁴ See Appendix 2 - section 135ANA. Parties who may take civil action include any person with an interest in the copyright of the broadcast, the copyright in any content of the broadcast and the channel provider who supplies the broadcaster with the channel for the broadcast.

serious consequences for the convicted person, the state and society generally. Once the criminal law is invoked, public resources are required for prosecuting the offence. Should the person be convicted the administration of the penalty, including any term of imprisonment, is the responsibility of the state. Given the above, governments must have sound reasons for criminalising activity.

86. The **sixth factor is how similar conduct is regulated, including in other Commonwealth legislation.** In general, theft or fraud offences under Commonwealth law have a direct Commonwealth connection. However, it is noted that the dishonesty offence with respect to obtaining a gain from a carriage service provider in section 474.2 of the Commonwealth Criminal Code referred to in the paragraph 57 of this paper is arguably similar.

87. While every country has its own policy reasons for creating criminal offences, it is also of some assistance to consider how the same activity is regulated in other countries. The conduct is criminalised in the United States (US), Canada, the United Kingdom (UK) and New Zealand (NZ).

88. The US has an offence covering various practices of ‘unauthorised publication or use of communications’ that states that no person who is not entitled to receive, shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information contained in it) for his own benefit or for the benefit of another not entitled to it.⁵⁵ The *US Communications Act of 1934* includes an offence for unauthorised reception of cable service. It states that no person shall intercept or receive or assist in intercepting or receiving any communications offered over a cable system, unless specifically authorised to do so by a cable operator or as may otherwise be specifically authorised by law.⁵⁶ In Canada, the unauthorised decoding of any encrypted subscription programme signal is prohibited under the *Radiocommunications Act*.⁵⁷

89. The UK *Copyright, Designs and Patents Act 1988* includes an offence of fraudulent reception of transmissions. The offence applies where a person dishonestly

⁵⁵ 47 U.S.C. 605.

⁵⁶ Sec. 633. [47 U.S.C. 553] The penalty for wilful violation of this provision is a fine of not more than \$1,000 or imprisonment for not more than 6 months, or both.

⁵⁷ Section 9(1)(1)(c).

receives a programme included in a broadcasting or cable programme service provided from a place in the UK with intent to avoid payment of any charge applicable to the reception of the programme.⁵⁸ The NZ *Copyright Act 1994* includes an offence of fraudulently receiving programmes. The offence applies where a person, with intent to avoid payment of any charge applicable to the reception of a programme included in a broadcasting service or cable programme provided from a place in NZ, receives such a programme.⁵⁹

Is there a basis for the Commonwealth to criminalise the activity?

90. The Commonwealth can legislate in areas where it has the constitutional power to do so. The Commonwealth clearly has power to regulate extensively in the areas of copyright and communications.⁶⁰

91. This paper has already explained that accessing a subscription broadcast, even without authorisation, does not breach the copyright in the broadcast. This is consistent with merely accessing other forms of copyright material. For example, it does not breach copyright to read a book, listen to a legitimate CD or watch a movie on a legitimate DVD.

92. Accessing a subscription broadcast without paying for it may be dishonest but the Copyright Act only criminalises such unauthorised dealings with copyright material where there is commercial advantage or profit involved. Criminalising activity carried out in a purely private or domestic context would be a departure from this policy. If the Commonwealth were to criminalise this particular activity concerning encoded broadcasts as a dishonesty offence it would effectively be distinguishing between dishonest dealings in relation to encoded broadcasts from dishonest dealings with other forms of copyright material. There would need to be sound policy justifications for making this distinction.

⁵⁸ *Copyright, Designs and Patents Act 1988* (UK) section 297. If found guilty of this offence the person is liable on summary conviction to a fine not exceeding 'level 5 on the standard scale' (£5,000).

⁵⁹ *Copyright Act 1994* (NZ) section 227. If found guilty of this offence the person is liable on summary conviction to a fine not exceeding \$5,000.

⁶⁰ Relevant powers under the Constitution would include section 51(v) (postal, telegraphic, telephonic, and other like services) and 51(xviii) (copyright).

93. One basis for distinguishing unauthorised access to encoded broadcasts from unauthorised access to other forms of copyright material is the scale of the unauthorised activity. Once access is gained to a subscription broadcast the recipient has continual access to the broadcast and all its underlying content - 24 hours a day 7 days a week. Assuming the unauthorised recipient has access to the full range of channels this is access to a significant amount of copyright material. Arguably, the continual nature and scale of the access may distinguish unauthorised access to a subscription broadcast from unauthorised access to other types of copyright material such as a film or a sound recording.

Question 1: Should it be a criminal offence under Commonwealth law to access and use a subscription broadcast without authorisation of the subscription broadcast provider if it is accessed and used in a purely private and domestic context?

Other unauthorised activities concerning subscription broadcasts

94. This part examines other unauthorised activities involving subscription broadcasts that are of concern to the industry. They are effectively unauthorised uses of a subscription broadcast by a subscriber. In all cases the subscription broadcast has been accessed with the authorisation of the subscription broadcast provider on the basis of a legitimate subscription. They concern what the subscriber does with the subscription broadcast after they have accessed it. None of these activities are covered by the civil remedies or criminal offences concerning encoded broadcasts in the Copyright Act because the subscription broadcast has been accessed with authorisation. This review is for the purpose of considering whether these activities ought to be criminalised under Commonwealth law.

95. These activities include the following:

- domestic subscriber relocation of reception equipment or distribution of the subscription broadcast to other parts of the subscriber's home for purely private and domestic purposes

- domestic subscriber relocation of reception equipment or distribution of the subscription broadcast to other parts of the subscriber's premises for commercial purposes, and
- subscriber distribution of the decoded broadcast to other premises.

Possible remedies under the Copyright Act

96. Depending on the circumstances of the distribution, it is quite possible that the distribution of the subscription broadcast would be a breach of the broadcaster's copyright in the broadcast⁶¹ as well as the various copyrights that may exist in the underlying content of the broadcast.⁶² Where this is the case the usual remedies and offences in the Copyright Act for copyright breaches may have some application.

Contractual remedy available

97. The subscription agreements between the subscription broadcast provider and the subscriber would ordinarily set out what the subscriber can and cannot do in relation to the subscription broadcast and the equipment provided to access the service and the consequences of not complying with the agreement. All activities above would likely breach the agreement between the subscription broadcast provider and the subscriber and a remedy for breach of contract would be available to the provider. However, the breaches are arguably of differing magnitude in terms of their impact and, because of this may warrant differing policy responses.

Factors to be considered in determining whether the criminal law should apply

98. The discussion earlier in this section regarding the factors to be considered in determining whether the criminal law should apply is also clearly relevant in relation to these unauthorised activities. However, the following additional points are made.

99. In relation to these unauthorised activities there are clear contractual remedies available. The subscription broadcast provider would likely have the legal right under the contract to enter the subscriber's premises to investigate the subscriber's activity

⁶¹ Section 87, Copyright Act. However it is noted, that the fact that a subscription broadcast is shown in a public viewing area, including commercial and licensed premises does not involve any breach of copyright (section 199).

⁶² Sections 31(1), 85 and 86, Copyright Act.

and recoup any loss incurred.⁶³ Once the breach has been detected and threats of legal action made, it is quite possible that the subscriber and subscription broadcast provider could reach agreement on appropriate damages without any need for the matter to be resolved through the court system.

100. By comparison, a law enforcement agency would have to obtain search warrants to fully investigate the activity and prosecute the subscriber through the court system. Criminalising any or all of these activities would effectively shift the cost of enforcement of the terms of a contract between private parties to the public purse.

101. The question in relation to each of these unauthorised activities is whether it is a matter that is more appropriately dealt with under the contract between the subscription broadcast provider and the subscriber or under Commonwealth criminal law. This requires determining whether or not it is appropriate to use public funds and public law enforcement resources as a remedy for an act that is essentially a breach of contract between private parties and for which an appropriate private legal remedy would be available. In some cases it may be. In other cases it may not. For this reason, further information relevant to each particular activity is provided below.

Distribution or relocation in same premises for purely private and domestic purposes

102. This activity would include the situation where a domestic subscriber, without authorisation, connects a device after the incoming subscription broadcast has been decoded so that the broadcast can be viewed in one or more locations in the home. For example, the authorised subscription broadcast connection is to the living area of the home but the subscriber splits the cable so that the broadcast can also be viewed in a bedroom.

⁶³ Under the FOXTEL Subscription Agreement a subscriber agrees to provide FOXTEL with access to the subscriber's premises to enable FOXTEL to 'install, maintain, inspect or remove' FOXTEL equipment. It is expected that other subscription broadcast providers would have similar clauses in their subscriber contracts.

103. As an unauthorised use of a subscription broadcast it has been included in this paper.⁶⁴ However, it is clearly at the low end of the scale of unauthorised activities. While it may not be authorised under the agreement with the subscription broadcast provider, it does not harm others and any commercial loss to the provider is minimal. The subscription broadcast provider is receiving the correct subscription for the service received. The only loss to the provider would effectively be any profit from the fee charged by the provider for supplying and installing the necessary equipment.⁶⁵

Relocation or distribution in same premises for commercial purposes

104. This activity applies where a subscriber to a domestic service relocates the reception equipment or distributes the decoded broadcast to another area of the same premises that is used for commercial purposes. It may also be a public viewing area. This may occur, for example, in a hotel where a subscriber's premises is used for both domestic and commercial purposes - the hotelier subscribes to a domestic service but relocates the equipment or distributes the broadcast to a public viewing area to avoid the higher subscription fee for the more appropriate commercial service. Alternatively, the subscriber may split the signal so that it can be simultaneously viewed in the domestic and commercial areas of the premises.

105. This activity is clearly of a more serious nature than the first activity. Similarly with the first activity the question is whether it is a matter that is more appropriately dealt with under the contract between the subscription broadcast provider and the subscriber or under the criminal law.

106. In relation to a contractual remedy it is noted that there can be limitations with relying on contract as an appropriate remedy for this activity for all parties affected by it. In the hotel example above, the party that suffers the loss because the hotelier has not subscribed to the more appropriate commercial service may not be a party to the

⁶⁴ For example, the FOXTEL Digital Subscription Agreement [at http://www.foxtel.com.au/digital_terms.htm] contains prohibitions on moving or interfering with FOXTEL equipment without their consent. The Agreement also states that the service recipient is only permitted to use the service 'for private viewing purposes' at the recipient's home address.

⁶⁵ For example, according to FOXTEL's Pricing Summary as at February 2005, the fee for installing a new subsequent outlet without a set-top unit and without a telephone line is \$150: www.foxtel.tv/Digital_Pricing_Guide_Feb05.pdf.

contract and has limited scope to obtain a remedy under contract law. This may render a contractual remedy less appropriate. However, as it is a known risk, particularly where there are both private and public areas within the same premises, it arguably should be able to be dealt with in the subscription broadcast contract.

Subscriber distribution of subscription broadcast to other premises

107. This activity applies where a subscriber (either to a domestic or commercial service) decodes an encoded broadcast and then distributes the broadcast to one or more other premises. Distribution effectively means that control of the subscription broadcast has been passed on to others. While it may just be distribution to a single neighbour, it could also be to many others. Each of the parties to whom it is distributed may themselves distribute it to others. Because of this possible flow-on effect this activity is clearly the most serious of the three unauthorised use activities by subscribers.

108. As already noted, this activity would clearly breach the agreement between the subscription broadcast provider and the subscriber and a contractual remedy would be available. In cases where there has been distribution to only one other person it may be considered appropriate to deal with the matter by way of contract. However, once distributed there is no control over what the recipient does with the broadcast. Further distribution activity may occur. The subscription broadcast provider has no contractual remedy against the recipients of the distributed broadcast. This could effectively mean that a contractual remedy is inadequate to deal with this distribution activity.

109. The fact that the Copyright Act currently contains an offence concerning the distribution of a subscription broadcast in section 135AS(1B) indicates that the Government considers the distribution of a subscription broadcast to be a serious matter. It is arguably so regardless of who is responsible for the distribution and whether or not the subscription broadcast has been accessed with or without authorisation.

Question 2: Should it be a criminal offence under Commonwealth law for a subscriber to a subscription broadcast service

(a) to distribute a subscription broadcast or relocate reception equipment within the subscriber's premises for purely private and domestic purposes

(b) to distribute a subscription broadcast or relocate reception equipment supplied for a domestic subscription broadcast service to another area in the subscriber's premises for commercial purposes, and/or

(c) to distribute a subscription broadcast to other premises.

Appendix 1 - Protection for subscription broadcasts under the Copyright Act

This appendix provides information about how subscription broadcasts are currently protected under the Copyright Act. It provides information about the rights of copyright owners, particularly in relation to broadcasts, and how those rights are enforced.

Copyright owners' rights

Copyright law gives creators and other producers or investors certain exclusive economic rights, for a limited time, to deal with the products of their creative endeavours. The Copyright Act divides these creative endeavours into two separate categories:

- original literary, dramatic, musical and artistic works (collectively called 'works') and
- sound recordings, cinematograph films, television (TV) and sound broadcasts and published editions of works (collectively called 'subject matter other than works').

In relation to a TV or sound broadcast (whether a subscription or free-to-air service, or whether transmitted by satellite or cable) the copyright ownership can be complex. First there is the copyright in the broadcast itself which may be live-to-air or a broadcast of material pre-recorded by the broadcaster or material owned by others.⁶⁶ There may be separate copyright in the underlying visual images and sounds in the broadcast and in some cases, there may be many separate copyright owners.

The owner of the copyright in a TV or sound broadcast is the maker of the broadcast.⁶⁷ In simple terms, the owner of the copyright in a cinematograph film is the maker of the film and the owner of a sound recording is the maker of the sound recording.⁶⁸ There may also be separate copyright ownership in the various components of a film and sound recording. For example, there may be separate copyright in the script, the literary work on which the script is based, cartoon drawings, individual sound recordings and music works, the musical score and so on. Separate copyright ownership rules also apply in relation to broadcasts of live performances.⁶⁹

The exclusive rights under copyright include the right to copy, publish, communicate to the public (eg make available online) and publicly perform the copyright material. The Copyright Act also grants copyright owners moral rights.⁷⁰ A broadcast is

⁶⁶ Under section 91 of the Copyright Act copyright subsists in a TV or sound broadcast made from a place in Australia under the authority of a licence or a class of licence under the Broadcasting Services Act 1992; or by the Australian Broadcasting Corporation (ABC) or the Special Broadcasting Service Corporation (SBS). For licensed broadcasters see www.aba.gov.au/.

⁶⁷ Section 99. See also subsection 22(5).

⁶⁸ Sections 97 and 98. See also sections 22, 23 and 24.

⁶⁹ See section 22 and other provisions concerning performances and performers in the Copyright Act.

⁷⁰ These are the rights of attribution of authorship, a right against false attribution of authorship and the right of integrity of authorship.

defined in the Copyright Act as a communication to the public delivered by a broadcasting service within the meaning of the *Broadcasting Services Act 1992*. Broadcasting is, therefore, part of the copyright owner's communication right.

As noted above, separate copyright exists in a broadcast and the broadcaster has exclusive rights concerning that broadcast. In relation to a television broadcast consisting of visual images and sounds, copyright is the exclusive right of the maker of the television broadcast to make a cinematograph film of the broadcast, or a copy of such a film; to make a sound recording of the broadcast, or a copy of such a sound recording; and to re-broadcast it or communicate it to the public otherwise than by broadcasting. For a sound broadcast, copyright is the exclusive right of the maker of the sound broadcast to make a sound recording of the broadcast, or a copy of such a sound recording; and to re-broadcast it or communicate it to the public otherwise than by broadcasting it.

Copyright owners sometimes use technological means to protect and enforce their rights. Encrypting a broadcast so that only authorised subscribers who have been supplied with a decrypting device can receive the signal is a means by which the broadcaster protects their copyright and the copyright in the underlying material in the broadcast.

Use of copyright material

While copyright covers acts such as copying of copyright material some acts are not affected by copyright. For example, merely reading a book, listening to a music CD or viewing a film on DVD does not affect the copyright owner's rights. This is the case even if the book, CD or DVD is a copyright infringing copy.

Similarly, receiving and viewing a television broadcast does not breach any copyright in the broadcast itself or the material being shown in the broadcast. This is the case whether the broadcast is a free-to-air broadcast or a subscription broadcast.⁷¹

Enforcement of copyright

Copyright is essentially a private right that is enforced under civil law. When a copyright breach occurs the copyright owner can seek redress against the person who infringed the owner's copyright. This may take the form of seeking an injunction to restrain an infringement occurring or continuing or damages as compensation for the infringement. The court has wide power to grant remedies for infringement of copyright.⁷² For example, the court may order payment to the copyright owner of any profit made by the infringer as a result of the infringement.

Although copyright is a private right primarily enforceable by private civil action, Parliament has deemed it appropriate for criminal offences to apply in some cases of copyright infringement and other activities in relation to copyright material. Most of those offences focus on activity involving infringing copyright material where it involves one of a number of activities that create or support a market in copyright

⁷¹ It may result in an infringement of copyright if, for example, the broadcast was recorded in some way.

⁷² See sections 115 and 116.

infringing material or where the person carries out the activity with the intention of obtaining a commercial advantage or profit. In addition, there is now a separate offence for significant copyright infringement. This deals with conduct resulting in copyright infringement where the infringement has a 'substantial prejudicial impact on the owner of the copyright and the infringement occurs on a commercial scale.'⁷³ In determining whether the infringement is on a commercial scale consideration must be given to the volume of infringing copies, the value of the infringing copies and any other relevant matter.

In the framing of the copyright offences involving various dealings with infringing copyright material⁷⁴ a clear policy distinction exists between activities involving infringing copyright material with some commercial context or of significant scale or value and infringing activities carried out by an individual in a purely private or domestic capacity. Enforcement action for copyright infringing activities by individuals in a private or domestic capacity is dealt with in civil courts.

In recent years the range of activities for which civil action may be taken has increased. The range of activities that constitute criminal offences has also increased. A person found guilty of an offence under the Copyright Act is punishable on summary conviction by a fine or, if considered appropriate by the court, a term of imprisonment. These changes, particularly as relevant to subscription broadcasts, are explained further below.

The Digital Agenda amendments

Significant amendments were made to the Copyright Act by the *Copyright Amendment (Digital Agenda) Act 2000* (the Digital Agenda amendments) to allow the creators of copyright material to take advantage of the new online technologies and promote access to copyright material online, in particular for cultural and educational institutions.

In addition to the creation of new rights such as the right of communication to the public, the Digital Agenda amendments added new civil remedies and criminal sanctions to the Copyright Act. These included new enforcement regimes in relation to devices and services used to circumvent technological protection measures (TPMs) and the intentional removal and alteration of electronic rights management information (ERMI). The Digital Agenda amendments also added new Part VAA to the Copyright Act that applied in respect of subscription broadcasts and included new definitions, and specific civil remedies and offences.

Notably, the offences relating to TPMs and circumvention services and devices do not involve dealings with infringing copyright material. They concern **access** to legitimate copyright material. These offences effectively acknowledge that copyright owners operating in the online environment have the right to protect their copyright through technological means and that certain unauthorised activity involving the means by which TPMs are circumvented ought to be proscribed. Consistent with the general policy referred to above, these offences focus on the making, importing,

⁷³ Section 132(5DB) and (5DC).

⁷⁴ See section 132.

advertising, commercial dealings with and distribution of circumvention devices and like activities regarding provision of circumvention services.⁷⁵

The actual use of a circumvention device or service is not proscribed. Accessing copyright material, even by using a circumvention device, is not a breach of copyright. However, the material accessed is covered by copyright. If the user were to copy, communicate or do any of the other acts with the copyright material accessed that is within the exclusive rights of the copyright owner without the authority of the copyright owner, then the user will have breached copyright. In this case, the usual civil remedies and criminal offences apply.

The same rationale was applied in relation to the offences in the Copyright Act concerning subscription broadcasts. The encoded broadcast offences focussed on the making, importing, advertising, commercial dealings with and distribution of broadcast decoding devices. The offences were not directed at punishing copyright infringing activity – they concerned access to copyright material (the encoded broadcast). Accessing a broadcast, including an encoded broadcast, is not a breach of copyright. But the broadcast itself and, in many cases, the sounds and visual images embedded in the broadcast, are covered by copyright and, if the user does an act that breaches that copyright the usual civil remedies and criminal offences apply.

Definitions of ‘encoded broadcast’ and ‘broadcast decoding device’

The Digital Agenda amendments included definitions of ‘encoded broadcast’ and ‘broadcast decoding device’ that form components of the criminal offences and civil remedies in the Copyright Act relating to subscription broadcasts.

An *encoded broadcast* is defined in the Copyright Act to mean:

- (a) a broadcast that is made available only to persons who have the prior authorisation of the broadcaster, and only on the payment of subscription fees (whether periodically or otherwise), or
- (b) a broadcast (other than a radio broadcast or a broadcast to which paragraph (a) applies) that is delivered by a commercial or national broadcasting service within the meaning of the *Broadcasting Services Act 1992*.

In the case of either (a) or (b) the definition also requires that access to the broadcast in an intelligible form is protected by a technical measure or arrangement (including a computer program). An example would be an encrypted broadcast.⁷⁶

A ‘broadcast decoding device’ was defined to mean a device that is designed or adapted to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster, by circumventing, or facilitating the circumvention of, the technical means or arrangements that protect access in an intelligible form to the broadcast.

⁷⁵ Some circumvention of technological protection measures is permitted in the Copyright Act for ‘permitted purposes’: see section 132(5F)-(5H).

⁷⁶ Section 135AL.

Criminal offences and civil remedies concerning subscription broadcasts

In summary, the Digital Agenda amendments made it a criminal offence to manufacture, import, sell, hire, trade, distribute, exhibit for trade or make available online, a broadcast decoding device. Although the amendments did not prohibit the personal use of such devices, a civil remedy was provided for the use of a decoding device for a commercial purpose.

All the criminal offences and grounds for civil action concerning unauthorised access to subscription broadcasts in Part VAA of the Copyright Act are based on or around the broadcast decoding device that facilitates unauthorised access to encoded broadcasts. An unauthorised set-top box used to access a subscription broadcast would constitute a 'broadcast decoding device'. Also, a legitimate set top box may become a 'broadcast decoding device' if, for example, it is adapted by the use of a pirate smart card to enable a person to access more channels than they are authorised to access under the terms and conditions of their subscription. A person who is convicted of an offence concerning an encoded broadcast is punishable by a fine of not more than 550 penalty units (ie \$60,500) and/or imprisonment for not more than 5 years.⁷⁷

As noted above, the Government adopted the view that the use of a broadcast decoding device, privately or otherwise, should not be criminalised. This was consistent with the Government's policy that the main threat to subscription broadcasters was not the single act of unauthorised reception by individuals, but rather the preparatory acts carried out by commercial companies, and the unauthorised use of such devices to promote commercial activities.⁷⁸

Amendments implementing the Australia-United States Free Trade Agreement

The AUSFTA included specific obligations in respect of protection of encrypted program-carrying satellite signals in Article 17.7. While the Digital Agenda amendments went some way to meeting those obligations, further amendments to the Copyright Act were required that strengthened the protection for subscription broadcasts. The amendments extended the range of activities that constitute an offence, the range of actions subject to civil action and the range of parties who may take civil action. These amendments should have a corresponding deterrent effect on subscription broadcast piracy. These amendments came into effect on 1 January 2005.

⁷⁷ Subsection 135AS(4).

⁷⁸ Senate, Revised Explanatory Memorandum to the Copyright Amendment (Digital Agenda) Bill 2000, item 104.

Appendix 2 - Current criminal offences and civil remedies in the Copyright Act concerning subscription broadcasts

The following table sets out the activities in relation to subscription (encoded) broadcasts that currently constitute criminal offences and for which civil action may now be taken under the Copyright Act.

(Unauthorised) activity	Criminal offenceⁱ	Civil actionⁱⁱ
Making a broadcast decoding device	Yes – ss 135AS(1) A person must not make a broadcast decoding device if the person knows, or is reckless as to whether, the device will be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.	Yes – 135AN Applies where: <ul style="list-style-type: none"> • broadcaster makes an encoded broadcast; and • without the permission of the broadcaster a person makes a broadcast decoding device; and • the person knew or ought reasonably to have known, that the device would be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.
Sells, lets for hire, or by way of trade offers or exposes for sale or hire, a broadcast decoding device	Yes – ss 135AS(1) A person must not sell, let for hire, or by way of trade, or with the intention of obtaining a commercial advantage or profit, offer or expose for sale or hire, a broadcast decoding device if the person knows, or is reckless as to whether, the device will be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.	Yes – 135AN Applies where: <ul style="list-style-type: none"> • broadcaster makes an encoded broadcast; and • without the permission of the broadcaster a person sells, lets for hire, or by way of trade offers or exposes for sale or hire, a broadcast decoding device; and • the person knew or ought reasonably to have known, that the device would be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.
Distributes (including by exporting from Australia) a broadcast decoding device for the purpose of trade, or for any other purpose that will affect prejudicially the broadcaster	Yes – ss 135AS(1) A person must not distribute (including exporting from Australia) a broadcast decoding device with the intention of trading or	Yes – 135AN Applies where: <ul style="list-style-type: none"> • broadcaster makes an encoded broadcast; and • without the permission

	obtaining a commercial advantage or profit, or with the intention of engaging in any other activity that will affect prejudicially a broadcaster if the person knows, or is reckless as to whether, the device will be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.	of the broadcaster a person distributes (including by exporting from Australia) a broadcast decoding device for the purpose of trade, or for any other purpose that will affect prejudicially the broadcaster; and <ul style="list-style-type: none"> the person knew or ought reasonably to have known, that the device would be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.
Exhibits a broadcast decoding device in public by way of trade	Yes – ss 135AS(1) A person must not exhibit a broadcast decoding device in public by way of trade or with the intention of obtaining a commercial advantage or profit, if the person knows, or is reckless as to whether, the device will be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.	Yes – 135AN Applies where: <ul style="list-style-type: none"> broadcaster makes an encoded broadcast; and without the permission of the broadcaster a person exhibits a broadcast decoding device in public by way of trade; and the person knew or ought reasonably to have known, that the device would be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.
Imports a broadcast decoding device into Australia for the purpose of: <ul style="list-style-type: none"> selling, letting for hire, or by way of trade offering or exposing for sale or hire, the device; or distributing the device for the purpose of trade, or for any other purpose that will affect prejudicially the broadcaster; or exhibiting the device in public by way of trade 	Yes – ss 135AS(1) A person must not import a broadcast decoding device into Australia with the intention of <ul style="list-style-type: none"> selling, letting for hire, or by way of trade, or with the intention of obtaining a commercial advantage or profit, offering or exposing for sale or hire, the device; distributing the device for trading or with the intention of obtaining a commercial advantage 	Yes – 135AN Applies where: <ul style="list-style-type: none"> broadcaster makes an encoded broadcast; and without the permission of the broadcaster a person imports a broadcast decoding device into Australia for the purpose of: <ul style="list-style-type: none"> selling, letting for hire, or by way of trade offering or exposing for sale or hire, the device; or distributing the device for the purpose of trade, or for any other

	<p>or profit, or for engaging in any other activity that will affect prejudicially a broadcaster;</p> <ul style="list-style-type: none"> • exhibiting the device in public by way of trade or with the intention of obtaining a commercial advantage or profit; <p>if the person knows, or is reckless as to whether, the device will be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.</p>	<p>purpose that will affect prejudicially the broadcaster; or</p> <ul style="list-style-type: none"> • exhibiting the device in public by way of trade; and • the person knew or ought reasonably to have known, that the device would be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.
<p>Making a broadcast decoding device available online to an extent that will affect prejudicially the broadcaster</p>	<p>Yes – ss 135AS(1) A person must not make a broadcast decoding device available online to an extent that it will affect prejudicially a broadcaster; if the person knows, or is reckless as to whether, the device will be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.</p>	<p>Yes – 135AN Applies where:</p> <ul style="list-style-type: none"> • broadcaster makes an encoded broadcast; and • without the permission of the broadcaster a person makes a broadcast decoding device available online to an extent that will affect prejudicially the broadcaster; and • the person knew or ought reasonably to have known, that the device would be used to enable a person to gain access to an encoded broadcast without the authorisation of the broadcaster.
<p>Unauthorised use of broadcast decoding device to access encoded broadcast</p>	<p>If used in commercial context – Yes - ss 135AS(1A) A person commits an offence if</p> <ul style="list-style-type: none"> • a broadcaster makes an encoded broadcast; and • the person uses, or authorises the use of, a broadcast decoding device to gain access to the encoded broadcast; and • the access is gained without the authorisation of the broadcaster; and • the person uses, or authorises the use of, the device by way of trade or with the intention of obtaining a 	<p>Yes – 135ANA Applies where:</p> <ul style="list-style-type: none"> • broadcaster makes an encoded broadcast; and • a person uses, or authorises the use of, a broadcast decoding device to gain access to the encoded broadcast without the authorisation of the broadcaster; and • the person knew, or ought reasonably to have known, that the broadcaster had not authorised the person to gain access to the broadcast by so using, or authorising the use of, the device.

	<p>commercial advantage or profit.</p> <p>If used in a purely domestic context – No.</p>	
<p>Distribution of encoded broadcast accessed without authorisation</p>	<p>Yes – ss 135AS(1B)</p> <p>A person commits an offence if</p> <ul style="list-style-type: none"> • a broadcaster makes an encoded broadcast; and • a broadcast decoding device is used to gain access to the encoded broadcast; and • the access is gained without the authorisation of the broadcaster; • the person distributes (including by communicating), or authorises the distribution of, the broadcast that has been accessed by the device; and • the person knows the broadcaster had not authorised the access to the broadcast; and • the distribution affects prejudicially the following persons: <ul style="list-style-type: none"> (i) any person who has an interest on the copyright in the broadcast; (ii) any person who has an interest in the copyright in any content of the broadcast; (iii) the channel provider who supplies the broadcaster with the channel for the broadcast. 	<p>Yes – 135ANA</p> <p>Applies where:</p> <ul style="list-style-type: none"> • broadcaster makes an encoded broadcast; and • a broadcast decoding device is used to gain access to the encoded broadcast without the authorisation of the broadcaster; and • a person distributes (including by communicating), or authorises the distribution of, the broadcast that has been accessed by the device; and • the distribution affects prejudicially a person who may bring an action under ss 135ANA(3) and • the person knew that the broadcaster had not authorised the access to the encoded broadcast.
<p>Receipt of encoded broadcast accessed without authorisation</p>	<p>If received and used in commercial context – Yes - ss 135AS(1C)</p> <p>A person commits an offence if</p> <ul style="list-style-type: none"> • a broadcaster makes an encoded broadcast; and • a broadcast decoding device is used to gain access to the encoded broadcast; and • the access is gained 	<p>Yes – 135ANA</p> <p>Applies where:</p> <ul style="list-style-type: none"> • broadcaster makes an encoded broadcast; and • a broadcast decoding device is used to gain access to the encoded broadcast without the authorisation of the broadcaster; and • a person receives the

	<p>without the authorisation of the broadcaster; and</p> <ul style="list-style-type: none"> • the person receives the broadcast that has been accessed by the device; and • the person knows the broadcaster had not authorised the access to the broadcast; and • the person uses, or authorises the use of, the broadcast by way of trade or with the intention of obtaining a commercial advantage or profit. <p>If received and used in a purely domestic context – No.</p>	<p>broadcast that has been accessed by the device; and</p> <ul style="list-style-type: none"> • the person knew that the broadcaster had not authorised the access to the encoded broadcast.
--	--	---

ⁱ Criminal offence provisions do not apply in relation to anything lawfully done for the purposes of law enforcement or national security by or on behalf of the Commonwealth or a State or Territory; or an authority of the Commonwealth or of a State or Territory (s 135AS(2)).

ⁱⁱ Civil remedies do not apply in relation to anything lawfully done for the purposes of law enforcement or national security by or on behalf of the Commonwealth or a State or Territory; or an authority of the Commonwealth or of a State or Territory (s 135AN(2)).