Study on the use of conditional access systems for reasons other than the protection of remuneration, to examine the legal and the economic implications within the Internal Market and the need of introducing specific legal protection

Report

presented to the European Commission

by

N. Helberger
N. A. N. M. van Eijk
P. B. Hugenholtz

Institute for Information Law
(IViR)
University of Amsterdam

Preface

The study, commissioned by the Directorate-General for Internal Market and Financial Services (DG XV) of the Commission of the European Community, offers an analysis of the use of conditional access systems for other reasons than the protection of remuneration interests. The report also examines the need to provide for additional legal protection by means of a Community initiative, such as a possible extension of the Conditional Access Directive. The report will give a legal and economic analysis of the most important non-remuneration reasons to use conditional access (CA), examine whether services based on conditional access for these reasons are endangered by piracy activities, to what extent existing legislation in the Member States provides for sufficient protection, and what the possible impact of the use of conditional access is on the Internal Market. Furthermore, the study analysis the specific legislation outside the European Union, notably in Australia, Canada, Japan and the US, as well as the relevant international rules at the level of the EC, WIPO and the Council of Europe.

This study was written by Natali Helberger and Dr Nico A. N. M. van Eijk at the Institute for Information Law (IViR), University of Amsterdam under the supervision of Professor P. Bernt Hugenholtz (project leader). The economic part of the analysis was written in co-operation with Berlecon Research GmbH, Berlin, Germany as expert for the economic questions. Furthermore, the Institut de l'Audiovisuel et des Telecommunications en Europe (IDATE), Montpellier, France was consulted as a subcontractor.

The opinions expressed in this Study are those of the authors and do not necessarily reflect the views of the European Commission.

Amsterdam, April 2000

Executive Summary

Conditional access (CA) is, generally spoken, a technical solution which allows its user to control and secure access to electronically transmitted services and contents as well as to determine the conditions under which access is granted.

Until now, CA was mostly associated with pay-TV services and access control as means of ensuring the remuneration of such services.

To protect services which use CA against pirate activities which may hamper the development and viability of such services, the Conditional Access Directive (CAD) was adopted which presently is in the process of implementation in most of the Member States. The Directive focuses exclusively on conditional access devices serving the remuneration interest of service providers. Doing so, the Directive does not provide for protection of conditional access devices where they serve other interests of service/content providers.

The European Commission commissioned the presented study to examine whether, apart from remuneration reasons, other, non-remuneration reasons to use CA exist which may deserve additional legal protection.

For the purpose of this study, we used the following definition of the notion of "non-remuneration reason". "Non-remuneration reason" means any interests which are not directed upon the provision of any form of direct financial payment by the receiver in return for the provision of a service by the service/content provider.

The study identifies a variety of such non-remuneration reasons for which providers of broadcasting and information society services use CA devices. The different reasons range from the use of CA in order to comply with contractual and statutory obligations and marketing and advertising strategies to security aspects, but also indirect remuneration reasons. With each of these reasons, the decision to implement CA is based upon valid economic and legal considerations which reflect the economic value of CA devices used for non-remuneration reasons. The economic value of CA is determined by the economic profitability of CA devices as solution for legal or market requirements, in some cases even by the existence of the service itself. Furthermore, CA devices can be also means of developing alternative financing models of services, for example where used for targeted advertising or to ensure indirect remuneration interests which are probably not covered by the CAD.

At the moment, no significant data are available on how the market for services which use CA devices for non-remuneration reasons will develop. Current market trends, however, suggest a further growth of the market for such services. On the other hand, the increased use of CA devices itself probably will have some impacts on the Internal Market such as implications for market structures and competition, access to services and content, choice of offers and further interests of consumers.

One observation of this study was that it is probably still to early to predict seriously how the market will develop and what effect an increased use of CA devices will have on the market. It is also not possible to assess to what extent piracy of services which use CA devices for non-remuneration reasons will play a role for the provision of such services within the Internal Market. There is, however, some reason to believe that providers of such services

will be exposed to a comparable extent to pirate activities as this was already the case for pay-TV providers. The same is true for the question whether CA devices used for non-remuneration reasons are endangered by piracy activities.

As long as there is no immediate piracy problem, however, which would seriously hamper the development of CA use for non-remuneration reasons, there does not seem to be direct need for action.

The analysis of national and international regulations shows, that the protection of free services under national laws is still incoherent and various. Only few Member States included services which use CA devices for non-remuneration reasons, when providing for specific legislation. Where national regulations do so, the majority of such regulations is designed with traditional broadcasting services in mind; only few laws also deal with access controlled information society services. Due to a lack of case law, it is also not clear to what extent protection may be completed by the application of general laws. The situation probably will not change once the CAD has been implemented into national laws. This is since, until now, no country was reported planning to exceed the Directive by also protecting the use of CA for non-remuneration reasons.

As a result, the use of CA devices for non-remuneration reasons is exposed to considerable legal uncertainty while excluded from the scope of the CAD. Whereas no reasons could be identified which would principally justify such an exclusion. Furthermore, the distinction as made in the CAD between remuneration and non-remuneration reasons raises serious concerns as to the efficiency and applicability of the Directive itself.

Therefore, the issue of protection of the use of CA for non-remuneration reasons could be treated as part of the general review of the CAD (Article 7 of the CAD). This would allow a coherent and systematic analysis of the need for further Community action, bearing in mind the economic value of CA devices where used for non-remuneration reasons and also taking into account possible side-effects of an extension on the Internal Market.

As the study has revealed, the use and protection of CA for non-remuneration reasons is part of a far broader context of interests involved with various different implications for the Internal Market and the interests of third parties concerned. Presently, it is still too early to assess the possible impact of CA use on the Internal Market. A serious estimation, furthermore, would require an extensive research which goes far beyond the scope of this study. A general review of the CAD should take into account the complexity of the issue and take the opportunity for further, more extensive research in order to assess the impact of CA use on the general market structures, competition and the interests of the market players, particularly consumer interests.

Probably only some of such aspects would fall directly into scope of aspects which are treated by the CAD. Whereas further aspects may fall in the scope of other, already existing EC initiatives, e.g. in the framework of the Standards Directive and the Television Without Frontiers Directive. Part of an general review of the existing legal framework for CA devices could be whether the existing regulations are still adequate or if further initiatives may be needed.

Research should also pay attention to possible direct and indirect effects of an extension itself on the market, for example on the general decoder market. Initiatives should not lead to a hindrance of either the general decoder market or technical development and encryption

research. When envisaging an extension, attention should be paid to this point and also to the definition of “illicit devices” under the CAD.

Furthermore, the opportunity should be taken to examine how to encourage innovation and further standardisation of CA devices which would enhance the general security of the use of such devices.

An extensive review would allow to observe development of piracy in this sector and to assess how national judges will deal with future cases concerning the circumvention of CA devices which are used for non-remuneration reasons, and whether the protection under existing national specific and general laws is sufficient. By then, probably the draft Copyright Directive will have been adopted which would allow to also examine to what extent the provisions of Article 6 of the draft Copyright Directive could complete the protection of the use of CA for non-remuneration reasons.

If the result of such an observation reveals that the use of CA devices for non-remuneration reasons will increase as expected and that the sector will experience considerable problems with piracy, an extension of the Directive could be an appropriate solution to improve the legal situation of free CA services, but also to enhance the general efficiency and practicability of the Directive.

In case the European Commission decides against an extension, however, a precise definition of the term of “remuneration” would enhance legal certainty and facilitate the application of the Conditional Access Directive.

Index

Preface 2

Executive summary 3

Index 6

List of Abbreviations 8

1. Introduction 9
   1.1 Introduction 9
   1.2 Working method 11
   1.3 Structure of the report 13
   1.4 Description of the scope of the study and definitions 15
      1.4.1 Scope of the study 15
      1.4.2 Other definitions 18
   1.5 Introduction to conditional access 20
   1.6 Users of conditional access devices 23
      1.6.1 Introduction 23
      1.6.2 Broadcasting services 23
      1.6.3 Information society services 25
      1.6.4 Other services using conditional access 25
      1.6.5 Conclusions 26

2. The European Market 28
   2.1 The use of conditional access for non-remuneration reasons 28
      2.1.1 Contractual and statutory obligations 28
      2.1.2 Marketing and advertising strategies 30
      2.1.3 Security aspects 31
      2.1.4 Indirect remuneration reasons 34
      2.1.5. Conclusions 35
   2.2 Trends determining the market development 36
      2.2.1 Technical trends and factors 36
      2.2.2 Economic and business trends 39
      2.2.3 Consequences for the broadcasting sector 40
      2.2.4 Consequences for the sector of IS services 40
      2.2.5 Conclusions 41

3. Impact of conditional access use on the Internal Market 42
   3.1 Introduction 42
   3.2 Impact on market structure and competition 42
   3.3 Impact on technological progress 45
   3.4 Impact on consumers welfare and choice 46
   3.5 Conclusions 53

4. Problems with and related to piracy 55
   4.1 Piracy of conditional access devices used 55

4.2 Forms of pirate activities 57
4.3 Consequences of pirate activities 57
4.4 Cross-border aspects of piracy 58
4.5 Conclusions 59

5. Legal protection of conditional access services 60
5.1 International regulations 60
5.1.1 Introduction 60
5.1.2 Council of Europe 60
5.1.3 WIPO 60
5.1.4 European Union 61
5.1.5 Conclusions 63
5.2 Situation in the Member States 67
5.2.1 Introduction 67
5.2.2 Protection of free conditional access services 68
5.2.3 Structure of legislation 70
5.2.4 Notion of remuneration 72
5.2.5 Non-remuneration reasons protected 72
5.2.6 Services protected 73
5.2.7 Unlawful activities 74
5.2.8 Sanctions and remedies 75
5.2.9 Protection under general laws applicable 77
5.2.10 Transfrontier aspects 78
5.2.11 Third parties' interests 79
5.2.12 Additional legislation planned 86
5.2.13 Conclusions 87

6. Conclusions and recommendations 89
6.1 Conclusions 89
6.2 Recommendations 92

Annex I - Reports on international regulations and country reports
Annex II - Questionnaire to service providers
Annex III - Questionnaire to national correspondents
Annex IV - Questionnaire to consumer organisations and interest groups
Annex V - Questionnaire to providers of conditional access devices

List of Abbreviations

AEPOC = Association Européene de Protection des Oeuvres Cryptées

API = Application Program Interface

AUP = Acceptable User Policy

CA = Conditional access

CAD = Conditional Access Directive (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or of, conditional access, OJE L 320, 28.11.1998, p. 54)

CDPA = UK Copyright, Designs and Patents Act 1988

DTTV = Digital Terrestrial Television

ECT = European Community Treaty

ECHR = European Human Rights Convention
EPG = Electronic Program Guide

GUID = Global Unique Identifier

IS services = Information society service

MMDS = Multi Microwave Distribution System

TAC = Finish Telecommunications Administrative Centre

OPTA = Dutch Onafhankelijke Post- en Telecommunicatie Autoriteit (Independent Authority for Post and Telecommunications)

UWG = German Gesetz des Unlauteren Wettbewerbs (Unfair Competition Law)

US = United States of America

WCT = WIPO Copyright Treaty

WPPT = WIPO Performers and Phonogram Producers Treaty

1. Introduction

1. 1. Introduction

In recent years, broadcasting and information society services (IS services) have been making ever-increasing use of conditional access devices. This trend is expected to gather pace as the market for these services develops. The conditional access device (CA) provides the user with a technical facility which allows him to determine who has access to electronically-distributed services and under which conditions.

However, users and providers of conditional access systems are becoming increasingly exposed to attempts to circumvent this technology. As already indicated in the Green Paper on encrypted services, a flourishing piracy industry is manufacturing and marketing various forms of decoding devices which enable unauthorised persons to access services and content. Moreover, specific legislation on the protection of conditional access devices is in force only in a few Member States. In order to improve the legal situation of providers of broadcasting and IS services, the European Commission has recently drafted and adopted a Directive on the legal protection of services based on, or consisting of, conditional access (CAD).[1]

This Directive introduces a common standard of legal protection for conditional access devices. However, it focuses exclusively on conditional access devices that serve the remuneration interest of service providers and makes no provision for CA devices that serve other interests. Safeguarding remuneration interests is, however, only one of many reasons why a service/content provider may wish to control access to content and services. Accordingly, those who use conditional access devices for other reasons may still be exposed to piracy and will find only fragmentary and unharmonised protection (if at all) under the national laws.

The European Commission has responded to this situation by commissioning the present study on the use of conditional access systems for reasons other than the protection of remuneration. This study will examine the legal and economic implications within the Internal Market and the need for specific legal protection, such as an extension of the CAD.

As formulated by the Commission, the aims and objectives of the study were to provide:

- a legal and economic analysis of reasons for using conditional access techniques other than for safeguarding remuneration
- a prognosis of the impact of conditional access services that use conditional access for such purposes, particularly:
  - an evaluation of possible market developments and increase of services that use conditional access techniques for reasons other than to safeguard remuneration interests
  - an analysis of the impact of the development on the Internal Market, consumer choice and consumer access to services from other Member States
  - an evaluation of the economic value that service providers derive from the use of conditional access techniques
- a summary of national legislation and case law on the legal protection of services that use conditional access for reasons other than to safeguard remuneration, including:
  - the current national legislation in the 15 Member States of the European Union and

[1] Directive 98/84/EEC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, OJE L 320, 28.11.1998, p. 54.

  - the US, Canada, Japan and Australia as well as
  - international regulations at the level of EC, WIPO and Council of Europe and
- recommendations on possible future initiatives, as well as on aspects which might be relevant for drafting specific regulations on the legal protection of conditional access systems insofar as they serve purposes other than safeguarding remuneration.

In compliance with these objectives, the study focuses first on service providers which do not require direct remuneration in return for the service they provide. Although our research showed, that pay-TV providers may also use CA devices (additionally) for non-remuneration reasons, their purpose is still primarily to ensure remuneration interests and they therefore already fall under the CAD. On the other hand, the general interests in the use of CA differ in the case of providers of services which are not directly remunerated. Therefore, situations in which CA devices are used to provide free-of-charge services are particularly suited for an examination of the reasons and economics of the use of CA for other interests.

However, the pay-TV providers have generally more experience of the use of CA than the free-of-charge services – which also explains why we have taken account of their experience. The higher knowledge level can be explained by the fact that CA technology is relatively new and was initially applied mainly by certain online services and pay-TV providers in order to ensure that they received remuneration for their services.[2] Particularly in the beginning, the initial costs of implementing CA techniques were relatively high and therefore profitable only for a small number of providers. Today, however, the cost of CA devices is falling steadily. As a consequence, small service providers and providers of free CA services—which do not gain direct revenue from the application of CA techniques—are also becoming increasingly interested in the opportunities offered by these techniques. With the growing use of satellite broadcasting and, more recently, the introduction of digital technologies, the demand for conditional access systems is also increasing among free-of-charge CA broadcasting providers. On the other hand, this also may be true for IS services, where the costs of implementing a CA device are generally lower, given that it consists mostly of a software application.

Services with no economic value, such as beneficial services, are of less interest for this study.

Following the approach of the CAD, we made no distinction as to whether a particular reason for using conditional access is applied by a broadcasting or an IS service provider, since in most cases the reason mentioned may be true for both. If this is not the case, it will be pointed out in the analysis.

It should be noted, that the use of CA devices by providers of free CA services (particularly free-of-charge broadcasting services) is still in its infancy, which may be the reason that there are still few data available and that the level of experience and knowledge even among concerned parties is still relatively low. The assessment insofar is based upon the observation of current tendencies and developments in the market for broadcasting and IS services, interviews with interested parties, experiences already made in the pay-TV sector, research and own expertise.

[2] First implementation of CA in the field of pay-TV services can be traced to the mid 1980s in Europe with the launch of premium analogue Pay-TV channels (such as Canal Plus in France) or analogue multi-channel satellite packages (such as BskyB in the UK).

1. 2. Working method

For the purpose of the study, four work packages have been defined:

- Work package 1: Analysis of reasons to use CA other than remuneration reasons
- Work package 2: Prognosis of the impact of conditional access services using CA techniques for such purposes
- Work package 3: Summary of the applicable national legislation and case law on the legal protection of services using CA for other reasons than to ensure remuneration
- Work package 4: Recommendations on aspects which might be relevant when drafting specific regulation on the legal protection of conditional access systems as far as they serve other reasons than ensuring remuneration.

The work in all four work packages was performed on the basis of desk research, observance of recent market developments in the sector of broadcasting and information society, experiences from previous research, we performed in this field and other existing expertise. A further source of necessary information was a qualitative survey and the performance of interviews for which we approached selected represents of

- providers of broadcasting and IS services (commercial and public service broadcasters, providers of subscription television services, providers of IS services)
- a selection of providers of CA devices as a service in its own right
- a comprehensive selection of European and national consumers associations which are representative of each member state and
- selected national and international interest groups.

For this purpose, we designed four questionnaires to service providers, providers of conditional access as a service in its own, consumers organisations and interest groups which served as basis for the survey and the interviews The fourth questionnaire has been designed to be sent to national correspondents in each of the countries examined in order to facilitate the gathering of information on national specific legislation. The text of the questionnaires can be found in Annex II, III, IV and V to this study

The objective of the questionnaires was to obtain information on conditional access devices used for non-remuneration reasons, particularly

- to gather information on the use of conditional access techniques for non-remuneration reasons
- to evaluate possible market developments of conditional access devices and the increase in the number and types of services that can use conditional access
- to evaluate the impact of these developments on the functioning of the Internal Market (impact on competition, on consumer choice and access to contents/services provided from other Member States)
- to assess the extent to which conditional access devices used for non-remuneration reasons are threatened by piracy
- to analysis the existing legal protection of conditional access devices as well as the impact of such legislation on the Internal Market
- to assess whether and, if so, to what extent there is a need to introduce additional legal protection for service providers using conditional access and for providers of conditional access as a service in its own right.

The information gathered was used for the analysis within all four work packages.

Work package 1 comprised the identification and analysis of other reasons to use CA then to ensure remuneration. The work on this package included the precise definition of the term remuneration/non-remuneration interests. The evaluation and analysis of reasons to use CA was based mainly on a comprehensive survey of existing services using CA, the outcome of the survey and interviews with selected represents of both broadcasting and information society service providers, content providers and providers of conditional access systems as a service in its own right.

Work package 2 dealt with the economic prognosis of the potential market development of services using CA for non-remuneration reasons and the possible impact of these developments on the Internal Market and its market players. Based on concrete examples of selected providers of broadcasting and IS services using CA for non-remuneration reasons, the second work package lead to a legal and economic analysis of the most important non-remuneration reasons for which service providers use CA. Furthermore, we made a first assessment of the economic value of CA and identified the main trends which drive the development of CA systems using CA for non-remuneration reasons on the basis of which a first prognosis on possible market developments was given. This work package also dealt with the possible impact of such services on the Internal Market and its market players, particularly competitors and consumers. Furthermore, it was examined to what extent the use of CA devices for non-remuneration reasons is endangered by piracy in Europe.

Work package 3 included the analysis of the existing specific legislation and case law on the protection of CA services for the 15 Member States of the European Union and, additionally, the USA, Canada, Australia and Japan. Main objective of this working package was to examine to what extent national laws protect services using CA for non-remuneration interests and what the structure of such legislation is. On the basis of a comprehensive analysis of existing legislation we draw conclusions on the current state of protection of services using CA for non-remuneration reasons in- and outside of Europe. This chapter also paid attention to the question of whether Member States adopted additional rules with view of third interests such as public, consumers or market interests involved in the use of CA devices. Secondly, this work package comprised an analysis of existing and pending relevant initiatives on the level of the EC, WIPO and the Council of Europe.

To collect relevant legislation and case law and to gain the necessary information for the analysis, we collaborated with national experts in each of the Member States examined. Additional interviews with selected authorities, lawyers and consumer authorities served the purpose of further analysing existing national regulations as well as the effects of such regulations on the position of consumers, services and content providers and involved third parties.

Work package 4 focused on the preparation of the final conclusions and recommendations.
In this final part of the study, conclusions were drawn from the results achieved in this and the other three work packages and recommendations were formulated with view to possible future Community initiatives.

1.3. Structure of the report

The study is divided into six chapters. The first chapter includes the general introduction to the study, the executive summary and the description of the structure and methodology. It then defines the exact scope of the study and the relevant definitions used in this report. This is because the CAD does not provide any definition of the term "remuneration" or "non-remuneration reasons" whereas the general wording of the Directive leaves room for several interpretation to what may be covered. Thus, precise definitions are needed in order to avoid difficulties in delineating the scope of the investigation and to maintain consistency with existing Community initiatives in this field. Finally, chapter one looks more closely at the characteristics and functions of conditional access since these ultimately determine the purposes for which the technique can be used and introduces the major groups of market players who use CA devices for non-remuneration reasons.

Chapter two will analyse from a legal and economic perspective the main non-remuneration reasons for using CA. Secondly, it will provide a first assessment of the possible further development of broadcasting and IS services that use CA for reasons other than to safeguard remuneration. On the basis of the economic analysis, first indications will be given of the possible economic value of CA devices for non-remuneration reasons for and the impact of services using such devices on the Internal Market. By doing so, chapter two, together with chapter three, provides a first indication of whether services using CA for non-remuneration reasons are of relevance for the Internal Market.

Chapter three gives a first assessment of the possible implications of the use of CA for non-remuneration reasons on the Internal Market. Here, aspects will be identified which may be relevant when drafting specific regulation on the legal protection of CA for non-remuneration reasons. Chapter three should be read in context with chapter 5.2.11. of this study *(Situation in the Member States – third parties' interests*).

Chapter four examines to what extent services already using CA devices for non-remuneration reasons are exposed to piracy activities which may hamper the provision of these services. The threat of piracy may be a first indicator for the further need of Community action.

Chapter five addresses the question of how far these services are already protected by existing national and international regulations. The provisions in Australia, Canada, the US and Japan will also be described in order to give an idea of the legal situation outside the Community. The country reports and the reports on the current and pending international initiatives can be found in Annex I to this study.

The examination of existing national legislation shows to what extent the present legal protection of directly-remunerated services using CA is sufficient and where further harmonising of Community initiatives may be needed. Furthermore, the analysis has also been conducted with a view to the question of where the Member States include the protection of non-remuneration interests and whether this has lead to significantly different legal solutions. The European Commission has already concluded that this may be a possible

argument against the treatment of remuneration and non-remuneration reasons in one regulation.[3]

Other regulations in this field are discussed insofar as they have been adopted by the Council of Europe and the EC and bearing in mind that Member States would have to implement such regulations in their national laws where they may complete the protection of those services that use CA for non-remuneration reasons. The same may be true for proposals pending at the level of WIPO and the EC. Other initiatives which are not particularly relevant to the protection of CA services, but nevertheless deal with other aspects of the use of CA are discussed where necessary.

The analysis is followed by chapter six, the general conclusions and recommendations for future Community initiatives in this sector to, where necessary, improve the legal situation of services using CA for non-remuneration reasons.

[3] European Commission Green Paper on the legal protection of encrypted services in the Internal Market, 6.3.1996, COM(6)76 – hereinafter termed „Green Paper"; p. 7: "This exclusion (of services encrypted for reasons other than ensuring the payment of a fee) is based on the fact that the general interests involved in the event of interception of these services ... differ appreciably from the general-interest objective threatened by the illicit reception of encrypted services as defined for the purpose of this Paper. As the difference has led to appreciably different solutions in terms of legislation both at national and international level particularly as regards action and the level of sanctions, the joint treatment of both problems is not justified."

1.4. Description of the scope of the study and definitions

1.4.1. Scope of the study

This study examines to what extent a need exists for additional Community action to protect broadcasting and information services which use CA devices for non-remuneration reasons not covered by the CAD. In other words, the scope of the study depends on the nature of the services covered by the CAD and which reasons for using CA are protected. In this respect, the Directive is open to some interpretation.

Article 2 (a) CAD defines protected services as any service "which is provided in return for remuneration and on the basis of conditional access".

The definition could, effectively, be broadly understood to cover all remunerated services using CA, including those which are indirectly remunerated such as advertisement and fee-based services. Insofar, the notion of "remunerated" could be understood as a merely distinctive criterion in the sense of Article 50 (previously 60) of the Treaty ("normally provided in return for remuneration") in order to exclude non-commercial services. As a consequence, the Directive may even cover free-of-charge services as long as they pursue any commercial interest in some form or other and based on conditional access. Furthermore, the articles of the Directive do not explicitly state which reasons for using CA fall under the CAD.

However, the recitals to the Directive make clear that the aim of the regulation is to cover all services where encoding is used to ensure payment of a fee (recital 5), i.e. those services which use CA in order to obtain the service provider's remuneration which ensures the viability of the services as opposed to those services which allow access free of charge (recital 6). Also the Green Paper, which preceded the CAD, focused on services "whose signal is encrypted in order to ensure payment of a fee".[4]

Both, the Green Paper and the CAD itself, refer to a functional relation between the use of CA and the receipt of remuneration for that service. We therefore assume that the CAD exclusively protects services using CA *in order* to receive remuneration for services such as pay-TV and certain IS services. Whereas all other services would fall outside the scope of the Directive.

The question of when the services use CA for remuneration interests depends on the definition of remuneration as applied in the CAD. The directive itself does not provide any precise definition of "remuneration". Remuneration could thus be understood as the payment which a service/content provider receives directly from the customer in exchange for a particular service or the transfer of:

- indirect financial interests involved in the provision of the service such as copyright fees, commission, brokerage

[4] European Commission Green Paper on the legal protection of Encrypted Services in the Internal Market, 06.03.1996, COM (96)76 – hereinafter termed "Green Paper on Encrypted Services", p. 6.

- public fees, advertising and sponsorship revenues[5] which do not stem form the actual receiver of the service and
- any economic value such as information and non-financial return services[6].

As can be concluded from the context of the CAD the concept of "remuneration interest" would first have to be examined in the light of Articles 49 and 50 ECT.

Article 50 ECT does not give a definition of "remuneration" with regard to services either.

The European Court of Justice has defined "remuneration" in the context of Article 50 as "any economic value in return for the provision of a service, generally paid between service/content provider and receiver."[7] Accordingly, remuneration is considered only as transfer of economic value which are made in return for the provision of a service. Indirect financial interests in the provision of a service, such as copyright fees, broadcasting fees, commission, brokerage are therefore not covered.[8] The same applies to the general interest to protect the investment, in, say, the creation of a database, by restricting/controlling access to the service. In this case conditional access devices may serve general economic interests which, however, are not provided in return for the provision of a service.

The payment method is apparently unimportant (e.g. e-cash, bank transfer, invoice, subscription fee). [9]

Normally, there is a provision of remuneration between the provider and receiver of the service.[10] Situations may, however, arise in which the remuneration is provided by a third party, e.g. revenues paid by the advertiser or a general contribution by the public such as a public broadcasting fee. This may also be an arrangement such as an electronic online catalogue where the service itself is offered free of charge, but the provider of the catalogue is remunerated by the advertiser. The European Court of Justice has stated elsewhere, that the remuneration for a service does not necessarily have to be paid by the receiver of the service.[11] Consequently, remuneration can also be the payment a service/content provider receives from a third party other than the consumer for the provision of a service. Conditional access devices, however, which are normally applied between service provider and consumer, will only indirectly serve remuneration interests in this case. For the purpose of this study, we will therefore consider "remuneration interest" in the sense of the Conditional Access Directive i.e. only as the provision of a payment which derives *directly* from the consumer.

It is questionable whether the term 'remuneration' refers exclusively to the payment a service/content provider receives for the provision of certain services, or whether the transfer of other goods of commercial value, in particular, information or return-services in kind, are also covered. Note that certain information, e.g. about the consumer, consumer behaviour etc., is increasingly gaining its own market value. The same may apply to certain return-services in

[5] See European Court of Justice, Case 155/73 (Sacchi), 30 April 1974, p. 409, 431; case 352/85 (Bond van Adverteerders), 26. April 1998, p. 2102, 2114.
[6] See particularly jurisdiction of the European Court of Justice in the context of Article 144 of the Treaty.
[7] European Court of Justice, Case 263/86 (Humble), 1988, 5383, 5388, paragraph 17.
[8] See also Conditional Access Directive, Amended Proposal for a European Parliament and Council Directive on the legal protection of services based on or consisting of, conditional access, COM(1998)332 final, OJE No. C 203, 30.06.1998; Explanatory Memorandum: Article 1 (g).
[9] See European Court of Justice, 1991, I/1979, 2016, paragraph 26.
[10] European Court of Justice, Case 263/86, ibid, paragraph 17.
[11] European Court of Justice, Case 352/85, ibid, paragraph 16.

kind.[12] Generally, however, it will be extremely difficult to assess how far non-financial remuneration has economic, i.e. market value. Moreover, the Conditional Access Directive apparently addresses the remuneration interest as an interest to preserve the economic viability of services.[13] Given the difficulties in determining the exact market value of certain information in such services, this interest will generally focus on the provision of financial return (as opposed to services that are free of charge).[14] This explains why we assume that the remuneration interest of service/content providers in the sense of the Conditional Access Directive generally focuses on remuneration in form of payment of a subscription fee, electronic cash, etc.

In conclusion, we define "remuneration" for the purpose of this study as the provision of a form of direct financial payment by the receiver in return for the provision of a service by the service/content provider.

In so doing, we have opted for a notion of "remuneration", which is probably narrower than in the sense of Article 60 of the Treaty ("normally provided in return for remuneration"). This is to avoid inconsistencies with the CAD and the Green Paper and to draw a clear distinction between remuneration and non-remuneration reasons, and hence, the subject of this study. Consequently, the study will deal with all reasons which are not connected with the provision of a direct financial payment by the receiver in return for a service.

Accordingly, "non-remuneration reason" means all other reasons which are not directed upon the provision of a form of direct financial payment by the receiver of the service in return for the provision of a service by the content/service provider.

On the basis of the aforesaid, we also consider services in the sense of the CAD, those which use CA devices for direct remuneration reasons, such as pay-TV services and certain IS services. Whereas we assume that all indirectly financed services, which are generally provided free of charge (e.g. public broadcasting services, advertisement-funded services), do not fall under the CAD – they will be the main focus of the study. Although we also take into account the experiences of pay-TV providers regarding the use of CA devices, they are not of primary interest to this study, since they are already covered by the CAD.

"Pay CA services" or "directly remunerated service" means any broadcasting or IS services which make the provision of the service conditional on the direct payment of remuneration.

"Free CA services" or "indirectly remunerated service" means any broadcasting or IS services which do not ask for direct remuneration but which are financed indirectly, e.g. by means of advertising revenues or broadcasting fees but may impose other requirements on the user, e.g. requiring him to accept on-screen advertisements or to provide personal information.

In this context it is worth mentioning that "free" services, though principally provided free of charge, does not necessarily mean that those services have no economic value of their own; and hence are services in the sense of Article 60 of the Treaty. Otherwise they would be of only limited interest to this study since they would not fall within the jurisdiction of the Communities and could not be subject to any further Community activities.

[12] Return services have been considered repeatedly as remuneration in the jurisdiction of the European Court of Justice with regard to Article 141 ECT.
[13] Conditional Access Directive, Considerations, Note 6,
[14] See Conditional Access Directive, Amended Proposal, Explanatory Memorandum, Article 1, paragraph (b).

As the Court has decided repeatedly for broadcasting services, the transmission of television signals is subject to the rules of the Treaty relating to services.[15] The Sacchi decision concerned public and advertisement broadcasts and, thus, can be interpreted in a sense that the Treaty provisions on services also cover such as indirectly financed services. We have already referred to the Court Decision 352/85 (Bond van Adverteerders),[16] where the Court ruled that Article 60 does not require that the service be paid by those for whom it is performed, but also covers services which are e.g. paid by advertisers.[17] As Advocate General Warner explained in his comments on Case 62/79 (Debauve),[18] television broadcasting can be financed in different ways. Some broadcasting organisations are financed " wholly out of the proceeds of licence fees paid by viewers, others rely wholly on advertising revenues; and still others look partly to the one and to the other... The method of financing particular broadcasting organisations or particular broadcasts cannot be relevant for the answer to this question (i.e. if the Treaty applies to television broadcasts). The decisive fact is that television broadcast is normally paid for, i.e. remunerated in one way or the other."

Even if these decisions were ruled with broadcasting in mind, the argumentation in the case of IS services probably would not be very different.

This means that, for the purpose of this study, services which do not, in principle, receive direct remuneration are also suitable objects for the analysis, provided they have their own economic value and are provided in an economic environment.

1.4.2. Other definitions

For the purpose of this study and in accordance with the CAD, "conditional access" is defined as 'any technical measure or arrangement whereby access to a service in intelligible form is made conditional upon prior authorisation'.'[19] Like the Conditional Access Directive, the study will not distinguish between various conditional access devices or determine which technique is most suitable to serve as a reason for using conditional access, but will focus on the different purposes the technique may serve.

"Conditional access devices" mean 'any equipment or software designed or adapted to give access to a protected service in intelligible form'.[20]

"Television broadcasting" is understood as the 'initial transmission by wire or over the air, including that by satellite, in unencoded or encoded form, of television programmes intended for reception by the public'.[21]

---

[15] European Court of Justice, Case 155/73 (Sacchi), ibid, p. 409, 431; Case 52/79 (Debauve), ibid, p. 833.
[16] Ibid, p. 2131.
[17] See also the opinion of Mr Advocate General Mancini, delivered on 14 January 1988, for this case, p. 2102, 2114: „ ... the participants in the broadcasting, transmission and reception of a signal – the broadcaster, ... – pursue an economic interest or, in other words, that the supply of the service has an economic aspect. ... the supply of services does not case to be economic in nature where ... no transfer of money takes place between the broadcaster and the viewer."
[18] European Court of Justice, Case 62/79 (Debauve), 18. March 1980, 833, opinion of Mr. Advocate General Warner, delivered on 13 December 1979, p. 876.
[19] Article 2 (b) of the Conditional Access Directive.
[20] Article 2 (c) of the Conditional Access Directive.
[21] Article 2 (a) of the Conditional Access Directive and Article 1 (a) of Directive 89/552/EEC of 3 October 1989 on the co-ordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities, OJ L 298 , 17.10.1989, p. 60.

"Radio broadcasting" means ‘any transmission by wire or over the air, including by satellite, of radio programmes intended for the reception by the public’.[22]

"IS services" are defined as: any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.[23]

[22] Article 2 (a) of the Conditional Access Directive.
[23] Article 2 (a) of the Conditional Access Directive and Article 1 (2) of Directive 83/189/EEC of 28 March 1983 laying down a procedure for the provision of information in the field of technical standards and regulations, as last amended by Directive 94/10/EEC, OJ L 100, 19.4.1994, p. 18.

1.5. Introduction to conditional access

Article 2 b of the Conditional Access Directive (CAD) defines conditional access as “any technical measure and/or arrangement whereby access to the protected service in an intelligible form is made conditional upon prior individual authorisation”.

The definition indicates the two key features of CA – the possibility:
- to exercise control over the access to a service or content which is transmitted electronically
- to control the conditions under which access is granted.

From the first days of its implementation by pay-TV providers in the mid 1980s, electronic access control was clearly understood as a means of billing and payment of services. In one of the former proposals for a CAD, conditional access was described as "any technical measure and/or arrangement whereby access to the service in an intelligible form is made conditional upon a prior individual authorisation aiming at ensuring the remuneration of that service."[24] And even now, some national laws consider encoded services only as those which use CA devices in order to ensure remuneration.[25] The same understanding can be found among providers of services themselves.

The aim of this study is to ascertain whether it is necessary to see CA in a broader context. However, in order to do so, it is necessary to examine more closely what CA is and to determine the specific functions by which it is characterised.

The main conditional access techniques which are currently supported are:
- password devices
- encryption devices.

Evaluating and filtering devices are also increasingly used in the Internet domain, mainly to prevent undesirable material from being delivered to minors, but also for other applications, such as the secure delivery of professional documents. " Push technologies" in the Internet domain could possibly also be assimilated into access control since, on the basis of this technology, content or material is sent only to selected receivers. In the longer term, devices based on biometrics will also be increasingly used to implement conditional access, particularly within the framework of banking services or any other activity which involves authentication of users, certification of parties and integrity of data.

For the broadcasting sector, a number of conditional access systems currently co-exist in the European market (Viacess (France Telekom), Mediaguard (Seca), Betacrypt (Betaresearch), na (Irdeto), Nagravision (Kudelski), Videoguard (News Data System), DigicipherII (General Instrument), Connax CA (Connax Telenor). Among these, a selection of systems such as Mediaguard and Viaccess dominate the market and are used by different service providers throughout Europe.[26]

Some of these providers also develop CA devices for the sector of IS services (e.g. Betaresearch). Currently, however, the development of CA devices for broadcasting services

[24] Amended Proposal, Article 2b.
[25] E.g. Australia, Canada, France, see country reports.
[26] IDATE, Development of Digital Television in the European Union, Reference Report 1998, commissioned by the European Commission (DG XIII), p. 69.

still takes place separately from the development of CA devices for IS services. This is also to do with the structure of CA devices for both fields. In the field of IS services, the recipient of the service is at first principally unknown. Asymmetric systems are therefore required, for example, on the basis of a public key or a password. As the subscriber is already known in the case of CA for broadcasting services, simpler, not necessarily asymmetric systems may be sufficient, such as the encoding or scrambling of a signal by the service provider.

However, the process of convergence of transmission channels could also favour the development of universal CA devices suitable for both broadcasting and IS services (e.g. integrated set top boxes), considering that both services may be transmitted via the same transmission lines.[27]

Current existing CA technologies consist basically of software or data, codes, keys etc. designed to make the access to content or a service conditional upon prior authorisation. Producers of CA devices stated that nowadays the main focus of CA is on software rather than hardware. Although the hardware of e.g. a smart card itself provides some functionality, the 'device' may be realised in software rather than in hardware. In particular in the field of IS services, CAs are designed to run on a PC and therefore, in this particular market segment, the design of CA is even exclusively concentrated on software development.

Software can be adapted and could be designed to do different things at different times. In technological terms, a single CA system that would serve all kinds of reasons simultaneously or at different times is not inconceivable. This may indicate that CA devices are characterised by a functionality which is principally independent of any particular purpose the device may ultimately serve.

However, two main functions of CA devices are evident:
- control function
- security function.

As to the control function, CA devices are designed to control access to content or services which are transmitted in an electronic environment and to determine the conditions under which such access is granted.

Whereas the marketing of tangible goods is based upon actual transfer of ownership, intangible information products cannot be transferred in the traditional sense. Consequently, new solutions were needed for 'packaging' information. These had to be designed to allow service providers sufficient control over electronically distributed information and material. Particularly, where new transmission means with broader coverage emerged, such as satellite distribution or the transmission of digitised signals via the World Wide Web, CA is one way of regaining control over the target and means of transmission which are increasingly transcending traditional territorial boundaries. The control that is achieved is not a control over the transmission methods but control over who may access a service/content and under which conditions. This goal can be achieved e.g. by providing only selected persons with the means to access (through the smart cards and encryption key or password).

[27] It is expected that a new generation of decoders will be designed for handling a wide range of multimedia applications including Internet access via TV set or a PC. The new terminals will also ensure the management of all audio, video and multimedia TV and computer peripherals (VCRs, camcorders, hi-fi units, PC printers, game consoles, etc. IDATE, ibid, p. 67.

Part of the targeting function is also the prior identification of the user of a service, i.e. the person demanding access. The ability to control access to content and services is based on the possibility of establishing direct contact between the user who requests access and the service provider who authorises it. Authorisation necessarily includes identification of the requester. In this function, CA devices can be used to identify the user and establish, on the basis of a prior authorisation request, a personified relationship with the user of the service. This not only enhances the quality and security of the transaction but also allows the usage and the user to be monitored.

Since access is conditional upon prior authorisation, the controller of a CA device can, of course, also determine the conditions under which access is granted. Where CA devices are used to safeguard a remuneration interest, this condition is the prior payment of a fee. But service providers are free to determine other conditions, such as the provision of personal information or other services in return, certain characteristics of the user of a service (e.g. older than 18, citizen of a particular country etc.), or the acceptance of certain conditions laid down by the service provider (e.g. to receive commercial post or pay a fee to the holders of rights).

By identifying the potential user and determining the conditions under which a service can be received, service providers manage the relationship with the individual receivers of an electronically transmitted service. One could say therefore more generally that CA enables the management of intangible information products.

Closely linked to the control function is the security aspect of CA. Since conditional access devices make it possible to deny unauthorised parties access to content or information and communication systems, they can serve various security interests of service providers, not least security of communication and information networks, confidentiality, integrity and availability of data, privacy, protection of intellectual property as well as the security of financial transactions. Conditional access devices, in this context, will be applied either to protect actual content against unauthorised access or use, or to control access to systems and applications.

Security aspects of CA can play a role in different stages of the transmission of content – they can protect content or service for internal security purposes during the actual process of electronic transmission or in the domain of the service provider but they can also protect e.g. access to ensure the security of services (such as databases) which are in the domain of the service providers.

1.6. Users of conditional access devices

1.6.1. Introduction

This section provides an overview of different users of CA for non-remuneration reasons. As has been indicated already, the study will focus in the first place on the examination of situations in which CA devices are used by providers which do not require direct remuneration in return for service but use CA devices exclusively for non-remuneration interests. Although providers of pay CA services have indicated that the CA devices they have implemented *also* serve other purposes than remuneration interests, the general interests involved will however be different – the focus will generally still lay on safeguarding remuneration interests.

The study only looks at the use of CA in relation to commercial activities of service providers (as opposed to the use of CA in the context of non-commercial activities such as private homepages, communication etc. or exclusively internal purposes which are of only limited interest for the purpose of this study). In the following, examples are given of the most important types of services which have already implemented CA devices for non-remuneration reasons or are planning to do so in the short term.

1.6.2. Broadcasting services

Analogue satellite broadcasting
Among the group of providers of broadcasting services, first of all, providers of analogue satellite-transmitted broadcasts use CA techniques such as encryption. Given the satellite technical coverage (or footprint) and the increasing transmission capacities, satellite-transmitted channels generally have a broader coverage than is the case e.g. for terrestrial television. Significantly, transmission via satellite is often not restricted to a particular national territory but can be received in all countries of the footprint of the satellite. Satellite broadcasters may be confronted with the need to control the transmission received only in a particular area, for various reasons such as compliance with statutory or contractual obligations.[28]

Consequently, not only pay-TV providers but also a number of free CA service providers have already implemented CA devices when transmitting their programmes via satellite. In Denmark, for example, the Danish public broadcaster DR – was among the first free broadcasting services to implement CA devices. The second Danish public TV channel (DR1) broadcasts in encrypted form via satellite (analogue and digital, see below). No additional remuneration is asked for the provision of services, apart from the usual broadcasting fee. The Danish population was provided with the smart cards free of charge.

To give another example, the Austrian public broadcaster (ORF) is currently preparing to switch from unencrypted to encrypted satellite transmission of its programmes. The Austrian population is also provided with the smart card for free. The expenses are covered by the general broadcasting fee. Other states where free analogue satellite broadcasters use encryption techniques are the UK and Switzerland.

[28] Chapter 1.4.

In the case of analogue terrestrial and also cable broadcasting there will be generally less need to encrypt due to the restricted or easier to control transmission techniques.

Digital Broadcasting

One sector, where CA devices can be expected to play a particularly important role is digital broadcasting services. Digital broadcasting services most often use a special encryption system. Since the reception of digital television requires the existence of a set-top box on the consumer side, the step towards implementation of an additional CA system is not far away. Consumers must not even realise that a service has been encrypted (as long as no remuneration or other services-in-return are required) .

In the sector of digital broadcasting, we can also distinguish between providers of digital terrestrial, cable and satellite. Digital television was first introduced via satellite in a large majority of Member States.[29] As far as digital terrestrial broadcasting is concerned (DTTV), only a few Member States seem to have started upgrading their network of analogue terrestrial transmitters for enabling digital transmission.[30] For the time being, the market players which are strongly involved in the development of the digital market are rather pay-TV companies than free service providers, because direct financing from subscribers would facilitate return on investment.[31] However, also providers of non-directly remunerated services start to use CA techniques when providing their services.

For example, the first Danish public TV channel (DR1) is a terrestrial broadcaster whose programmes are transmitted in encrypted form and digitally (similar to DR2) for reception only within the Danish territory. As in the case of the DR2 programme, the service is not offered in return for additional remuneration. In the case of terrestrial and cable digital programme, [32] the wish to encrypt derives less from the need to restrict transmission to a certain territory since terrestrial transmission normally does not exceed national borders. However, in the context of digital broadcasting, a second aspect of CA comes into play – CA systems here are apparently not only used to control transmission but can also serve as means of providing and managing enhanced services, e.g. IS services on the Internet.

The Swedish public broadcaster (SVT1 and 2) is, for example, changing to digital distribution of programmes. Apart from providing programmes in digital format, SVT also indicated that it plans to offer, in the medium term, additional enhanced digital services on the basis of CA, such as an on-demand service, which would be offered to the audience for free. Also the Dutch public broadcaster, NOS, is currently changing to digital transmission techniques while, at the same time, implementing CA devices in order to provide interactive and thematic channels. In both cases, there are plans to provide programmes and additional offers for free, e.g. not in return for additional remuneration. Subscribers only have to pay an adequate fee for the smart card. This also shows that the provision of such new services is not necessarily

[29] In this context, it is interesting to notice that most digital services launched in Europe are restricted to serve one single national market. The reason for this can be found either in the transmission technique itself (e.g. terrestrial or cable digital television) or in legal and contractual obligations of service providers, e.g. with respect to content providers. The Nordic market constitutes an exception, since Finland, Denmark and Sweden are currently served by one and the same digital service (the profitability for a satellite platform in those „small“ countries with a common culture lies in a Nordic approach to the market). Whereas some other smaller markets are „“ dependent“ on neighbouring countries, such as is the case for the UK and Ireland, France and French-speaking Belgium or Luxembourg, Germany and Austria; IDATE, ibid, p. 32.

[30] IDATE, ibid, p. 21.

[31] IDATE, ibid, p. 51.

[32] According to a study performed by IDATE; digitisation of cable networks has not yet started in Ireland, Finland, Luxembourg, the Netherlands, Germany and Portugal, only marginally in Austria, IDATE, 20.

restricted to providers of pay-TV services but is also open, in principle, to indirectly financed public and commercial broadcasters.

Furthermore, encrypted free channels can also be found in the frame of multi-channels offers of some pay-TV providers. In the UK for example, SkyDigital and On-Digital are already bundling free CA services, such as BBC1, BBC2, ITV, and Channels 4 and 5. Another example is the digital programme bouquet of Canal+ in the Netherlands, which also includes free broadcasters.

1.6.3. Information society services

Contrary to the case of CA in the broadcasting sector, the implementation of such devices in IS services is often appreciably easier and cheaper, since the device generally consists only of software. As a result, it is difficult to provide an overview of the number of services on the basis of CA which develop alternative financing methods while using CA exclusively for non-remuneration reasons.

Because of this and the fact that the market for IS services is still a field in which the development of many new forms of IS services is possible, this study will concentrate on some selected examples of major groups of IS services which may use CA devices for non-remuneration reasons.

Again, the initial development has been driven by pay services using conditional access as a payment mechanism. A growing number of Web shopping sites aims at implementing systems for secure payments. Besides, Web sites where access is based on subscription are increasing as is the use of conditional access devices in the Internet domain. However, CA devices are also increasingly being used in the Internet for other reasons than securing payments or remuneration.

IS services on the basis of CA techniques are, in the first place, interactive (e.g. on-demand services, interactive computer games, etc.) as well as personalised one-to-one services and e-commerce applications. Secondly, services which are involved in the distribution of all forms of content via the Internet from information to software or books and music belong among the users of CA and use it as a security and management mechanism. Another type of information society service which is likely to use CA is based on databases, access to which is controlled and secured by means of CA. But CA techniques are also likely to play a crucial role where the service consists of provision of access to the Internet itself.

1.6.4. Other services using conditional access

It should also be mentioned that CA techniques are not only used by providers of broadcasting and information services but also providers of services which do not fall under either of these categories. For example, the Deutsche Telekom in Germany is planning to encrypt all programmes which are transmitted via its cable system (so called “ Grundverschlüsselung”). The precondition for transmission is prior encryption or consent to encryption by broadcasters. Although this is also done out of remunerative interests, a major reason is to increase the security of the transmission.

In the long term, the majority of companies in the tertiary sector or from the industry are also expected to implement CA devices in business-to-business services among others. In the framework of the 'net-economy', that is to say, in an economy based on networks, data protection and secure corporate information, CA devices are already used to restrict the use, processing and storage of 'strategic' or 'sensitive' information or content as well as to protect the company against illegal intrusion into the information systems. Besides, in the evolution towards the de-materialisation of the relationship not only between customer and enterprise but also among enterprises (business-to-business) themselves, increasingly “distant” services are implemented which offer personalised and secure direct communication.

Finally, CA devices are also used for private purposes, e.g. to secure an e-mail account or the exclusivity of a private homepage, security of communication or, importantly, protection of minors; broadcasters or providers of video-on-demand services introduce elements which allow parents to classify and to control, on the basis of conditional access devices, the programmes their children are permitted to watch.

1.6.5. Conclusions

Users of CA devices for non-remuneration reasons can be found both in the sector of broadcasting and IS services.

In the analogue broadcasting sector CA devices are particularly used by service providers which use transmission means with a natural broad coverage, notably satellite broadcasting services, which could theoretically be received in more than one country, but where the service provider wants to restrict transmission for various reasons (which will be explained further on) to particular areas or language zones.

In the case of digital broadcasting services a second aspect, apart from the control function of CA, comes into play, which is the use of CA in the framework of enhanced broadcasting and IS services which are offered from the same digital platform.

Apart from pay-TV providers, presently the number of broadcasters using CA devices seems to be relatively small. The trend is driven in the first place by public broadcasters who change their distribution infrastructure to digital services and defend their competitive position towards providers of remunerated digital broadcasting services. Commercial broadcasters still seem reluctant to implement CA devices. Again, this may have to do with the fact, that public broadcasters can usually fully or partly rely upon the general broadcasting fee to finance their investments and services, whereas commercial broadcasters depend entirely on the revenues from advertising and sponsoring contracts. At the moment, electronic access control seems to be detrimental to this objective since, until now, the number of households which are able to receive encrypted or access controlled services is rather limited.

This situation differs to some extent from the situation in the sector of IS services. One particularity of the use of CA devices in this field is the relatively low implementation costs since they mainly consist of software applications. As a result, smaller service providers and service providers which do not require direct remuneration, can also more easily afford to implement CA devices. Consequently, the fields where CA devices are also used for non-remuneration reasons are various.

Major fields of application of CA devices are services which distribute content by electronic as well as interactive means and one-to-one services and e-commerce applications.

2. The European Market

2.1. The use of conditional access for non-remuneration reasons

In this section it is looked into economic reasons for service providers to employ conditional access systems for other than direct remuneration purposes. As they do so to gain an economic advantage, the analysis also provides information on the economic value service providers can derive from the use of CA techniques when used for non-remuneration reasons.

This information about the economic value is presented in qualitative rather than quantitative form. First of all, almost no data exists on the use of CA systems for non-remuneration reasons. Secondly, the interviews conducted for this study have shown that CA systems are often used for remunerative and non-remuneration reasons at the same time. E.g., a pay TV broadcaster ensures payment by conditional access but at the same time makes sure that he contracts only with individuals he is allowed to contract with under terms and conditions of the content owner.

We have identified a total of four different reasons, why service providers do employ conditional access systems for non-remuneration reasons. Some of these are more often to be found with broadcasters, others are more often to be found with IS services. These factors are:

1. Contractual and statutory obligations
2. Marketing and advertising strategies
3. Security aspects as well as
4. Indirect remuneration reasons

2.1.1. Contractual and statutory obligations

Legal obligations are the most important reason for broadcasting services to use conditional access systems, as interviews with broadcasting companies have shown. These can take on two different forms: either a content owner has licensed the content to a broadcaster subject to the restriction of broadcasting to a certain area (contractual obligation), or different statutory regulations apply for the content (statutory obligations) in different regions or member-states. These obligations can force a broadcaster or ISS provider either to restrict access to a specific territorial area (e.g., a country or language area such as Germany, Austria, Swiss) or a specific audience (e.g., adults).

An example for such contractual obligations is the Danish broadcaster DR. DR provides free radio and television and is financed by license fee only. Its second TV channel, DR2, is broadcasted in encrypted form by satellite for reception in the Danish territory only. Smart cards are delivered to the Danish population free of charge. According to DR this encryption is necessary for copyright reasons, as DR acquires the right to distribute to the Danish territory only.

If DR wanted to distribute its contents in an unencrypted form, it would have to acquire additional usage rights, e.g. for Sweden or Germany, as these rights are typically issued on a territorial basis. With falling prices of CA systems, it can become economically useful to

distribute these devices by means of CA to the target group free of charge and to pay lower license fees for copyright-protected material. Obviously this trade-off is especially pronounced for small countries as a large area of a satellite footprint is outside their borders.

A reason for such contractual obligations might be the so-called "windowing strategy" in content marketing, which is rather often used for movies. To extract higher revenues, the release of movies in cinema, on video, on pay TV and on free TV usually follows a rather strict schedule. If a movie can be watched on free TV offered by a neighbouring country before it starts screening in the cinemas, the revenue loss can be considerable. In the worst possible case, a movie breaking even with a perfect windowing system can become a money loser without.

The main economic force behind these contractual obligations is revenue maximisation on part of the content owner through market segmentation. Market segmentation means that the whole market for such products is divided into comparatively homogeneous parts. By tailoring the products to specific wants and needs (e.g., preferred showing times), the consumers' willingness to pay (either in direct or in indirect form by enduring advertising) is generally higher. Therefore also the total revenue to be extracted from these products is larger. These economics are especially important for products like movies, where the (technical) distribution costs to additional users are negligible.

Broadcasters on the other hand can minimise cost by avoiding the payment for screening rights for a user group which is not their target group (e.g. the non-Danish population). As these obligations are contractual, they can be negotiated depending on the legal and technical framework.

From an economic point of view both, broadcasters and viewers profit from such arrangements. As costs are lower, profits tend to be higher for the broadcasters and prices for such services – either direct in the form of broadcasting fees and pay TV fees or indirect in the form of advertising hours to endure for free TV – tend to be lower.

Statutory obligations are different from contractual obligations, as they are external to the service providers. They might, e.g., result in territorial restrictions. This will be true particularly for the field of broadcasting. Here, the national rules on protection periods for cinema films, advertisement rules and youth protection will play a role. On grounds of public policy, in particular the protection of minors, public authorities may allow certain services (e.g. broadcasting channels aimed at adult audience) to operate on the condition that the service is encrypted so than reception can be limited to specific groups of viewers.[33] Where this is the case, providers of transitional services may face the need to ensure that their program cannot be received in a certain member state where the programme would conflict with national laws. But also time restrictions are still an important means of national broadcasting laws to enforce the aims of a policy on the protection of minors – although they are probably threatened to become increasingly ineffective due to time-shifts between different countries where a program is released. Whereas on the basis of access control, operators could ensure that a pre-scheduled program complies with the local time in different

[33] Under Article 22 of the Television without Frontiers Directive, for example, providers of broadcasting services are obliged to ensure that programs with possible harmful contents cannot be seen or heard by minors. The Directive names technical measures as possible means for achieving this goal. In this respect, conditional access techniques are possible means to prevent access of minors to harmful contents.

countries. To give another example, European pay-TV providers are obliged to observe a protection period as regards the showing of cinema films in television.[34]

The sector of IS services is less regulated yet. Here, particularly the national data protection and telecommunication laws impose obligations on service providers to ensure the security of communications and personal data by means of electronic devices such as CA.[35] In any case, these obligations are only economic in the sense that failure to obey them might jeopardise the existence of a service.

To summarise, although contractual and statutory obligations seem to be similar at first sight, a more close examination reveals that they are fundamentally different. Contractual "obligations" are, from the economic point of view, the result of profit-maximisation behaviour on part of the content and service providers. Statutory obligations are the result of different legislation in different countries.

2.1.2. Marketing and advertising strategies

Some services offered free of charge are financed by advertising. Most commercial TV channels belong into this group as well as the majority of content-based and community-based IS services. Some of these services use conditional access systems to identify their users and extract a higher advertising revenue due to better targeting, as in most cases advertisers are willing to pay more for an eye-contact the better focussed the user group is. A software company, e.g., would like to target their advertising to people deciding about software purchase in companies.

The German web based email service *GMX*, e.g., requires upon registration that the user reveals some demographic data about herself like sex, age, marital status, computer equipment, etc. It then uses password protection to identify this user and to show her advertising she is likely to be interested in. While the conditional access system in this case exists also for protection of privacy, it constitutes a major cornerstone in the business model of such services. The conditional access method chosen by these services is generally a password protection.

However, in the few years such services happen to exist, it turned out that many users are rather reluctant to use registration-cum-password services if the registration is *only* for advertising and targeting purposes. Less intrusive methods, like so-called cookies, are being used more often, as they do not require a user interaction. A somewhat decreased precision in targeting is offset with a higher number of users. Therefore, the use of conditional access systems *only* for the purpose to target advertising better, while promising in theory, is in practice much less relevant.

In CA based IS services the CA system often serves a dual purpose, just like in the *GMX* example, where it protects privacy. Thus, the crucial part in a business model of an IS provider trying set up a service financed by targeted advertising is to create a service, where users *want* to use a CA system. This is typically the case with personalised services, e.g., email, personal web calendars, or stock portfolio tracking. Information about the users

[34] Article 7 of Television without Frontiers Directive: „ Member States shall ensure that broadcasters under their jurisdiction do not broadcast cinematographic works outside periods agreed with the rightsholder."
[35] Several national telecommunication laws include a statutory obligation to ensure the security of communications including the implementation of means to prevent unauthorised access.

gathered upon registration can then be used to target advertising, which commands a premium over untargeted advertising.

A second, more traditional form of targeted advertising is the provision of niche services. These can be both, digital broadcasting and IS services, which specialise on a selected audience, i.e., on special tastes or interests of this group (e.g., sports channels, financial information services, children's channels, language channels, news channels, etc.). Specialised advertisers find their target group among the users of such services.

It is obvious that CA systems for such services will be employed for remuneration reasons. A different question is, though, whether it is useful to restrict the usage of such services to the target group if the services are advertising financed. Such a restriction would be a non-remuneration reason as defined for this study. In print media such restrictions do take place and are known as "controlled circulation".

Here the publication is only shipped to those who have identified themselves as belonging to the target group. In principle, this could also be done with IS services. However, the economics are different for digital services like broadcasting and IS services. For these, the marginal cost of accommodating an additional user is zero, whereas for print products an additional copy must be printed and shipped. This creates an incentive for print publishers to restrict circulation to the target group only.

Such incentives are much less pronounced for digital goods and services. If, e.g., an advertiser pays a service for economists to reach 10 thousand economists, he would not mind if in addition 5 thousand mathematicians see his advertisement – provided he does not have to pay for them. Likewise the IS service provider or broadcaster does not need to exclude these users. The only exceptions are, if these additional users do create costs, e.g. because copyrighted material included in the service is licensed on the basis of the number of users or because the additional users are so many that the technical IS service needs to be upgraded. But generally, there is no need for content or service providers in such a specialised service to install conditional access systems.

To conclude, the use of CA systems for targeted marketing alone is possible in theory but not very widespread in practice. If targeted marketing takes place in CA protected services, the CA system in most cases has another main purpose – at least from the users' point of view. In speciality or niche services CA systems for non-remuneration reasons are also not very important, as the economics of digital goods and services lead to a marginal cost close to zero for additional users and therefore no reason to exclude them. This argument does not apply, however, if, e.g. due to contractual obligations, the marginal cost becomes positive. This is more likely to be the case in broadcasting and ISS based on editorial content than with other IS services.

2.1.3. Security aspects

Especially in IS services, conditional access systems are often used for the protection of privacy and data. Such services do exist in different forms where the protection serves different needs: Obviously, one of the reasons for the German web based email service GMX to be password protected is, that nobody wants other people to read their emails. Without a conditional access system in use, this service would not be accepted by users and not sustainable as a business model.

In other services, the conditional access system is used to create trust into the security among users without which the service would also not be sustainable. An example would be auction services on the Internet like *eBay* or recommendation services like *dooyoo.de*. Here each user has a unique ID, which is used for rating his reliability, e.g. his delivery speed or the accuracy and usefulness of his recommendation. For such services it is essential that this rating system works and creates enough trust to make the service attractive enough to join. As with most IS services on the Internet, these are typically password-protected.

For these services the primary purpose of CA systems is the identification of users in addition to protection against unauthorised access. This aim distinguishes CA protected IS services from CA protection of pay TV and other broadcasters where the main aim is to exclude unauthorised viewers.

The main reason to employ CA systems in IS services, however, is the protection of privacy and data. E.g., in the IS service domain several networks of different users exist which protect the privacy of their communication over open networks by means of conditional access systems. Extranets between companies are the most obvious example. While most are private networks and not IS service in the strict sense, there does exist a reasonably large "grey area": For example, a couple of services provide "virtual office space" (e.g., *space2go* in Germany), where storage space for digital documents on the Internet is provided for workgroups and mobile workers. The stored data as well as the communication among users is encrypted as the documents are sent over the Internet. Without the possibility to restrict access, such a service would not provide a sustainable business model.

In a similar way, conditional access devices are used in the broadcasting sector for business TV, i.e., TV restricted to a certain company or group of companies. While these "programs" are often distributed via open networks – via terrestrial broadcast, satellite or Internet multicast – their content is sufficiently confidential to justify conditional access systems to protect the information from being seen by outsiders.

The reasons behind this data and privacy protection are a mixture between economic and legal interests. The main economic reason is plainly that a service, which cannot secure privacy and data protection, will have to bear drastic revenue losses and might even eventually go out of business. Compared to this simple story, the legal reasons to employ CA for data and privacy protection are more complicated:

Where service providers process personal data automatically, national data protection laws may even state the explicit obligation to implement appropriate technical and organisational measures to protect personal data against unauthorised access.[36] Corresponding provisions can be found, e.g., in Articles 4 and 5 of the ISDN Directive[37] and in national data protection or telecommunication laws.

[36] See also Article 17 Directive 95/46/EC of the European Parliament and of the Council of 25 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 30 – hereinafter termed „Data Protection Directive". See also Resolution (73)22 of the Council of Europe, section 5, 8, 9 as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Europ. T.S. No 108).

[37] Directive 97/66/EEC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of private telecommunication sector, OJE L 204, 30.10.1998, p. 1 – hereinafter termed „ISDN Directive".

For example, in the health care industry increased use of electronic information networks and services is made. Doctors, major health care purchasers, pharmaceutical industry, governments and insurance companies exchange electronically not only health care related information, including medical data on patients but offer also relevant services such as medical databases. Some Member States already adopted statutory provisions with the aim to ensure that access to medical data may be gained only by health professionals.[38]

The need to protect personal data may arise, for example, also where service providers request the input of personal information in the frame of an electronic subscription process, e.g. electronic registration for access to a hosting service. While consumers are subscribing to the service they will feed the system with personal data. In this case, again it is in the responsibility of the service providers to ensure the confidentiality of such data, for example by implementing encryption techniques.

A further economic and legal data protection issue is to secure the integrity of information and content. Unauthorised interception of information constitutes a serious threat for the integrity of information or contents where such are exposed to unauthorised manipulation or destruction during the transmission. While unlikely in the material world (e.g. with written communication) with electronic information exchange the correspondents (e.g. service provider and consumer) may rarely notice that the transmission of information has been intercepted or accessed. CA devices are traditionally one means to ensure the security of information. Encrypting of electronically processed information can be used to prevent unauthorised third parties form learning the content of messages or even altering, manipulating or destroying of contents.[39] This aspect is also important where service providers choose electronic transmission means for the delivery of purchased products such as software.

While security and integrity of data by means of CA systems is also crucial for financial transactions, this issue is more of importance for services that use CA for remuneration reasons.

Last but not least, the inner security of a service also plays a role for setting up CA systems. This is primarily an economic reason, as inner security is necessary to ensure the functioning of businesses: Protection might be needed internally against the input of incorrect or conflicting data by personnel, abuse of company owned facilities for personal purposes, manipulation, contamination etc. Consequently, service providers implement security measures against the personnel of the organisation in order to avoid unauthorised exploitation of business facilities, e.g. for personal purposes. By means of passwords, etc. organisations can ensure that access to certain facilities is granted only to authorised collaborators. Access can also be restricted to business times or limited to a certain amount of time or usage.

Also, there is an interest in protecting internal investment and property against unauthorised access from third parties outside the organisation. This is to prevent unauthorised access, interception, espionage, manipulation in/of contents as well as illegal intrusion of harmful contents such as viruses, conflicting data etc. which may threaten single applications and values as well as the availability and functionality of a whole system. In particular, where service providers „go online“ the vulnerability of systems to external assaults increases.

[38] See Data Protection Directive, Considerations, paragraph 42.
[39] See also Article 6 of European Commission’s Recommendation 94/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange, OJ L 338, 28.12.1994, p. 98.

Authorisation, in this situation, can help to prevent assaults when, for example, access to contents or networks and databases is made conditional upon prior identification or the passing of certain security checks by the security administrator (e.g. firewalls, routers, individual access control and identification, access control to dial-up servers etc.)

To conclude, a variety of economic and legal considerations make identification, privacy and data protection probably to the most important reason for IS services to employ conditional access systems for non-remuneration purposes. For broadcasting this necessity is less pronounced, although there do exist some similar situations (e.g. ensuring integrity of the news broadcasts).

2.1.4. Indirect remuneration reasons

While the most obvious forms of remuneration is the "pay-per-view" or "pay-per-use", the special character of information goods and services allows different forms of indirect or not-so-obvious remuneration, where it is not totally clear whether the CAD in its current form is applicable. As was already set out in the introduction, the notion of " remuneration" as used in the Directive is open to some interpretation.

The simplest case is a subscription service where a user pays in advance for gaining access to a service over a fixed period or up to a fixed usage amount or a combination of both. There is no direct remuneration, as the subscription service has been paid in advance.

The case becomes more complicated, if access to a broadcasting or information society service is granted upon subscribing to some other service. Subscribers of the printed version of *The Economist*, e.g., automatically obtain access to the *Economist*'s web site free of charge, which offers additional utility in form of an archive as well as supplementary information not included in the printed copy.

Another example is a broadcaster that offers encrypted free-of-charge digital broadcast of otherwise publicly available TV channels together with its pay TV program. It could be argued that protection of these "free" channels does not take place for remuneration reasons but to ensure that only those households are able to receive the free channels in digital form that are also subscribed to the pay-TV channels.

The economic reason behind these strategies is that "bundling" of services in many cases is more profitable for a content or service provider than selling the services separately. In such situations the distinction between parts of the bundle that are offered for remuneration and such that are offered as supposedly free add-on is only a marketing or sales decision.

A related reason for employing CA is to secure other forms of financing. E.g., a broadcaster might want to make sure that only those households are able to receive its program that have paid the general broadcasting fee. Alternatively a broadcasting service provider might distribute set-top boxes and keys to households that have paid the broadcasting fee. The latter is not the typical case of remuneration, as not the service or content provider employs the CA device but rather a third party.

To conclude, this "grey zone" of indirect remuneration is also a rather important aspect, which has been made possible by the character of information goods on the one hand and the possibility to employ conditional access systems on the other hand. As the number of TV

channels increases, it is most likely that bundling of goods will happen in broadcasting as frequently as it already happens for IS services.

2.1.5. Conclusions

Using CA devices to meet contractual obligations reduces costs especially for broadcasting service and content providers and allows for better exploitation of copyright-protected material by rightsowners. Moreover, meeting of statutory obligations (e.g. in the field of youth protection) can be essential to ensure the existence of the service.

For the sector of IS services, CA systems often provide the foundation of several IS services financed by targeted advertising. For users of services, however, the privacy protection is the main reason for agreeing to use CA systems and reveal personal data. Privacy issues are for economic and legal reasons the major incentive for ISS providers to use CA. Whereas targeted services based on digital goods have smaller economic incentive than traditional content providers to exclude users which do not belong to the target group.

Often, CA devices are used by service providers (pay CA services and free CA services) for more than one reason at the same time.

Concluding, CA devices where used by providers of broadcasting and IS services possess their own economic value which may range from the profitability to use CA for one particular reason up to ensuring the existence of the service itself. Whereas CA devices are essential to realise and protect that economic value.

CA devices are also used to restrict access to “free” add-ons to services and contents provided on remuneration basis (“bundling”). The strategy of bundling of services is also one example for a situation in which the distinction between the use of CA for remuneration or non-remuneration reasons is increasingly difficult.

2.2.Trends determining the market development

Several major trends and factors govern the use and adoption of conditional access systems, in broadcasting as well as for IS services. While in the following section technical and economic factors are analysed separately, this distinction is less clear-cut in reality. A standard, e.g., although primarily a technical factor, has immediate economic consequences (e.g. cost implications) and also influences the economic strategies businesses choose. Likewise, the increasing eagerness of companies for copyright protection has its roots in the technical reproduction possibilities of digital goods, which are much easier to copy than traditional goods. Thus, the following distinction should be seen more as determining the main elements of a trend than as an attempt of exclusive classification.

2.2.1. Technical trends and factors

A group of technical trends and factors can be identified that influence in one or another way the use of CA devices.

1. Increasing use of wide-area open networks
2. Better CA devices
3. Standardisation
4. Convergence of transport media

Increasing use of wide-area open networks
Most obvious is the influence of this technological trend for broadcasting. Initially, broadcasting was terrestrial, where the signal had only a limited reach. Thus, problems due to statutory or contractual obligations were negligible as the broadcast area could be controlled rather well. This changed with the advent of satellite broadcast, where the broadcast area – the footprint – is often much larger than the target region. To comply in this new technological environment with statutory and contractual obligations based on the old environment, conditional access systems are employed.

A similar trend can be observed for IS services. Originally, many of these (e.g. business information services like *Reuters*, *Bloomberg*, *Genios*) were only accessible via leased lines and sometimes even proprietary terminals. Here the conditional access was required by the fact that a leased line has to be installed by both parties. As these services moved to the Internet to make use of the cost advantages of open standards and networks, they had to accept a much higher vulnerability to attacks and intrusion. As a consequence, they had to employ different and better conditional access systems than before.

Better CA devices
With the increasing availability of cheap computing power, CA devices have become far more powerful over the recent years. Influenced by this trend as well as by the increasing use of wide-area open networks, the interest for cryptography has increased considerably in academia as well as in business. This has lead to a huge advancement in knowledge – both theoretical and practical – about access control methods and best practice access control for all kinds of applications. The change in cryptographic practice from secret keys – which are

prone to hacking – towards systems based on a pair of public and private keys illustrates this development best.

As this technological progress continues, the near future will see forms of CA that cannot be hacked by pirates as easily if they are used in a proper way. As can be seen already in expert discussions about electronic cash or the encoding of DVD systems, the technological debate will concentrate on the question whether an appropriate, tamper-resistant encryption technology has been chosen.

Thus, piracy will become more difficult than in the early days, where, e.g., descrambling devices used for broadcasting could be hacked relatively easily. The legal framework may have a considerable influence on this development. In the strictest form, where all kinds of piracy, be it for commercial or private purposes, will be considered illegal, the incentive for broadcasters to employ tamper-resistant encryption technology could be rather low.

One outcome of this technological progress is the increased computing power and functionality of CA devices in general and of smart cards in special, which has lead to an increased usage of these cards, also for conditional access. According to *Dataquest*, a consultancy, the chip card is the highest-volume electronics end product in the world with almost a billion cards sold in 1997. More than halve of these chip cards were smart cards. It is likely that, as also personal usage of smart cards increases further, they will increasingly be used for personal conditional access systems. The current household access systems (mostly set-top boxes) often operate already with smart cards.

Standardisation

Standardisation issues can have a considerable impact on the usage of conditional access devices. If common standards evolve or are set by a standardisation body and subsequently accepted and implemented by service providers, they can considerably decrease the costs of CA usage, since standards enable interoperability, i.e., the technical combination of arbitrary components from different manufacturers.

This is shown very clearly by the development of the Internet, which is based on common standards. Most IS services offered over the Internet are password protected if they use conditional access devices. The handling and transmission of passwords is standardised, which makes the use of this simple CA system very easy. If sensitive information, like personal data, company data or a credit card number is transmitted, the data transfer is also encrypted. This encryption is also based on common standards like SSL (secure socket layer), a simple certificate-based encryption and identification standard that is understood by all common Internet servers as well as browsers. By now this SSL standard forms the basis of most forms of e-commerce over the Internet. As this example shows, common simple standards, which are accepted by the majority, can lead to a fast and widespread use of CA systems.

As especially the broadcasting sector shows, standards can also become a tool for strategic behaviour if no commonly agreed-upon standard exists. The recent years have seen standard wars about set-top boxes in several member countries. To engage in such a war can be a reasonable strategy for companies, as such conditional access devices constitute bottleneck facilities. The company that controls this bottleneck has a monopoly for accessing the customer. In the case of set-top boxes, e.g., not very many families are willing to buy several different ones and change plugs for every channel change. If such a war lasts for a longer

time, it can considerably delay the introduction of new technologies and thus also the introduction of new services that make use of conditional access systems.

But also if a standardisation war is won by one party, the introduction of CA based new services will typically evolve more slowly than with open standards. Unless regulated in some way, the company controlling the bottleneck facility, e.g. the set-top box, has an incentive to exploit its monopoly position. Competing service or content providers would typically have to pay a license fee, if they wanted to access their customers through the competitor's bottleneck facility.

To conclude, it can be said that standardisation considerably influences the speed of adopting CA systems for IS services and broadcasting alike. If CA is largely based on open standards, adoption will be relatively cheap and take place quickly, as CA usage for IS services shows. If either monopolists control one part of CA systems or competing standards exist, the pace of adoption will be considerably slower.

Convergence of transport media

Traditionally broadcasting has happened via air, satellite or broadband cable. All these have been constructed as one-way communication means for some kind of one-to-many communication. On the other hand telephone and data communication lines have originally been used for unicasting or person-to-person communication. The Internet has changed this clear distinction and will further blur the differences.

It is now possible to access the Internet also via satellite and broadband cable, not only via dial-up or leased lines. For the providers of conditional access devices like set-top boxes for satellite or data reception this means that their bottleneck facility can become even more valuable, as it not only controls the access to broadcasting services but also to the Internet. Also its CA technology might be used for accessing CA controlled services on the Internet. For example, a cable operator might not only provide access to a variety of audio and video channels, but also to Internet services operated by the same content providers which are also access-controlled (*Disney,* e.g., is very active in both spheres, *Excite@Home* too).

The broadband Internet access via satellite is also an example of not-so-obvious conditional access for privacy reasons. As the downstream traffic is sent out via satellite, all receivers within the footprint can receive the signal. However, only the legitimate receiver should be able to decode the signal.

On the other hand the Internet is increasingly used for broadcasting. The major German news program, *Die Tagesschau*, e.g. is available as streaming video on the Web, the British *BBC* offers its radio programs as streaming audio and a German news-only channel, *ntv*, broadcasts the full program during work-days as streaming video on the Internet. Since the capacity of most Internet connections is still not very large, video is transmitted in a rather poor quality. Internet radio, however, has already become a widespread service in reasonable quality.

This convergence of the different transport media will provide challenges as well as opportunities for using conditional access systems. A special opportunity consists in the upstream channel available on the Internet that allows a better identification of the person or household accessing a CA restricted service.

2.2.2. Economic and business trends

While all the technological factors and trends mentioned above do have also economic implications, there are at least two aspects that are mainly economic or business:

Increasing copyright awareness and exploitation
Narrowcasting instead of broadcasting

Increasing copyright awareness and exploitation
While copyright protection has always been an issue, copyright owners have increasingly started to protect their right to exploit the economic value of their content. This has led to increasingly sophisticated marketing strategies for information goods. “Windowing” in the case of movies is one example of interest in the CA domain. Following this strategy, the rights owners typically start with screening the movie in cinemas, followed by video, pay TV and eventually free TV. Since different revenue-maximising starting dates exist in different countries (e.g., due to national film festivals, vacations or just habits), they try to segment their market as perfectly as possible. With an increasing number of content-producing enterprises going public, the pressure of the stock market will most likely force these companies to enforce their copyright more strictly than they have done so up to now to exploit their assets better than before.

A second reason for the increasing awareness of copyright owners of copyright infringement is the digital form of most of their works. It has never been so easy to duplicate copyright-protected material without loss of quality than it is with digital goods. Therefore content owners have an incentive to control access to their services so that potential copyright infringements can be detected more easily. An information society service, e.g., that is distributing photo images or music via the Internet might want to identify its users and provide each digital good with an individual watermark unique to this user. If these digital goods turn up on a CD-ROM later, the individual who has violated the copyright can be identified easily.

Narrowcasting instead of Broadcasting
Originally broadcasting has been a one-size-fits-all attempt to provide consumers with identical information and entertainment. Technological development as well as the business opportunities from providing information and entertainment better targeted to certain subgroups of the population has lead to an increasing number of narrow- or multicasters. These cast their program to a selected group of persons only. Conditional access is typically the means by which the information is restricted to certain groups.

The importance of this trend can be seen from the number of pay-per-view channels in Europe that has increased from only one in 1994 to a few hundred by now. The Internet further fosters this trend as it provides technical means to target information even better which makes narrowcasting also relevant for IS services.

This trend is not confined to digital goods. Also in the physical goods industry customisation and building-to-order have become rather important over the last years. Driving forces have also here been information technology as well as the business opportunities from being able to charge higher prices for customised than for standardised products.

2.2.3. Consequences for broadcasting sector

A major issue for broadcasters to cope with in the near future will be the convergence between the different transport media. Especially an extension of broadcasting (some) content via the Internet will further aggravate problems due to legal and contractual obligations. If such content is provided via the Internet, the covered region is not anymore the relatively small footprint of some satellite, but instead the whole world.

However, the convergence offers also advantages for broadcasters, as Internet technology provides different and additional technical solutions to set up conditional access solutions. Not only are these more standardised than in the traditional broadcasting sector, but they are typically software-based. They are therefore easier and cheaper to implement and replace in case of technical obsolescence. However, if not chosen appropriately, pure software-solutions might also be easier to pirate.

Furthermore, the Internet opens broadcasters new fields of activity and opens room for the development of new service offers on the basis of CA, for example in the field of narrowcasting.

A further trend of special importance to broadcasters will be falling costs and the technical progress in encryption devices.

Summarising, present trends – sinking costs for the implementation of CA devices, increased functionality and security of devices, increased awareness of the content industry, the use of wide-area-open networks, convergence and the possibilities to offer new forms of presenting broadcasting or offering additional IS services – indicate a possible future increase of the use of CA devices by broadcasters for non-remuneration reasons.

2.2.4. Consequences for the sector of IS services

As the number of Internet users increase further and a greater share of economic activity is taking place on the Internet, security will become an even larger issue than it is now. It is therefore expected that conditional access systems for IS services will improve quickly to keep pace with hacking attempts. Already now, most services can be made secure up to a relatively large degree.

More secure conditional access systems for IS services might also become available through an increased use of smart cards. While the combination of smart cards and PC is currently mostly used in special situations, it is likely that this will change in the near future, as smart card readers become cheaper and micropayment systems for the Internet evolve. These systems can then be used also for non-remuneration conditional access services, just like several adult services require a credit card number to enter the service, even if no payments are conducted.

Standardisation of several conditional access systems within the IS service domain is rather advanced, as already set out above. However, one field, where this is not yet the case, are payment services. If payment technology shall be used for CA solutions, this has also consequences for conditional access systems employed for non-remuneration reasons. Thus

IS service providers face similar challenges due to standardisation issues than broadcasters do.

A further challenge for ISS providers from the technical trends discussed above are the conditional access systems to be employed for Internet access via satellite or broadband. Information society service providers depend on effective security on the level of IP traffic.

Summarising, the legal and economic relevance of security and identification aspects on the Internet, the increased efficiency and functionality of CA devices as well as the tendency to targeted and customised service offers are clear market trends which suggest a further growth of the use of CA for non-remuneration reasons in the ISS sector.

2.2.5. Conclusions

Currently, several market trends seem to drive the increase of CA use for non-remuneration reasons.

Increasing use of open wide-area technologies like satellite and Internet requires the implementation of CA in order to protect services and to restrict services to target groups.

Technical progress in the field of CA systems advances quickly, which makes modern properly used CA systems much more difficult to pirate than older ones. Furthermore, standardisation of CA systems enables low cost CA solutions and this increases CA use. Whereas missing open standards can inhibit the market for CA use.

Technical progress also makes CA systems cheaper, which may foster a further increase of CA use.

Convergence of transport media enables new opportunities for CA protected services but also provides technological challenges.

Increasing copyright awareness will force service and content providers to employ CA solutions to protect rights owners interests.

Finally, technological development as well as business opportunities from targeting content and services will lead to an increasing use of narrowcasting instead of broadcasting, which requires CA solutions.

Summarising, the trends identified suggest an increased use of CA devices also for non-remuneration reasons in both the sector of broadcasting and information society services.

3. Impact of conditional access use on the Internal Market

3.1. Introduction

Two related questions are to be discussed in this section. The first question is, what impact an increasing use of CA devices for non-remuneration reasons has on the Internal Market. The second, somewhat different question, is what impact an extension of the CAD to include also such CA protected services would have. This distinction is an important one: as interviews conducted for this study have shown, CA systems *are* already used for non-remuneration reasons.

There are three major elements of the Internal Market that will be discussed here with respect to CA use for non-remuneration reasons, namely:

1. Impact on market structure and competition,
2. Impact on technical progress, and
3. Impact on consumer welfare and choice.

For these three items the analysis might lead to different answers for broadcasting and for IS services.

3.2. Impact on market structure and competition

The most obvious impact of CA use on market structure and competition in the broadcasting domain stems from the bottleneck character of CA devices in this domain. The owner of a set-top box has a monopoly in accessing the household where it is installed. This is well known to the content and service providers. More than half of those surveyed agreed that CA solutions can be used to modify competition in one's favour. Considering that those surveyed have no interest in answering this question honestly, this is a remarkable percentage.

The impact of this special character of CA devices on market structure and competition has already been extensively discussed in the context of pay TV and cable networks. However, with CA use for non-remuneration reasons this discussion gains further facets.

One is the access of, e.g., free TV broadcasts to CA devices owned and operated by pay TV services. The Standards Directive of the European Union,[40] which addresses issues of access to bottleneck facilities, obliges the owners of such facilities to grant other broadcasters access on a fair, reasonable and non-discriminatory basis. However, The Standards Directive was designed with digital pay-TV services in mind, as can be seen from the Recitals. It is very questionable whether its provisions also apply to providers of CA devices for free CA services which use CA devices for other reasons than to ensure remuneration. It is also unclear whether the obligations the Directive imposed on providers of CA devices also apply *in favour* of providers of free CA broadcasting services.

[40] Annex I, section 1.2.5.

Secondly, the Directive does not deal with the delivery of other, non-broadcast services, i.e. IS services supplied by broadcasters via CA systems. Nor does it deal with issues of CA control in the field of online activities of broadcasters or CA devices for IS services.

In the online sector, problems of standardisation will possibly be less focused on the standardisation of hardware or free access to decoder systems, but will occur in other constellations, e.g. the field of the compatibility of browsers and access to leading portals as well as the dominant position of market leaders in this field.

Apart from these two major concerns, the Standards Directive deals only partly with problems which may emerge in the growing market for pay *and* free CA services based on CA. There are still a number of open questions. We already mentioned the lack of standardisation in the field of payment systems. However, as it is beyond the framework of this study to discuss the provisions of the Directive, we concentrate on giving some further examples which may be of particular importance when also providers of free CA services begin to distribute their services on the basis of CA.

For example, the opposite scenario is more directly related to an extension of the CAD. If CA devices used for non-remuneration reasons will be better protected by legal instruments, the owners of such devices might start to engage in competition with pay TV broadcasters for ownership of the bottleneck facility. They can then try to derive revenue for letting other broadcasters access this bottleneck. Currently, such a strategy is rather risky, as CA devices used for non-remuneration reasons are not protected by the CAD. This makes them not suitable for use for remuneration reasons in addition to a non-remuneration use, as pirates could always claim that they only wanted to access the free service.

The extent to which a competition for the bottleneck and, eventually, the monopolistic use of the bottleneck (in this case: CA devices for non-remuneration reasons) distorts competition, depends very much on the openness of standards. If the bottleneck is not standardised or if the standard is a proprietary one, the monopolistic elements will be stronger than with open standards. This issue has already been extensively discussed in the domain of pay TV and cable TV regulation.

Another issue not covered by the Standards Directive but which may gain increasing importance particularly when providers of free CA services enlarge the number of CA services, are competitive issues in the context of EPGs and APIs. EPGs and APIs are crucial components of CA devices; they are designed to handle the increased offer of digital channels in a bouquet, and also to provide access to transactional services (pay-per-view and video-on-demand) and such IS services as interactive services (home-banking etc.), Internet access and electronic commerce generally. The use by free CA service providers of digital transmission techniques and CA services will increase the number of and competition between channels, and there is therefore a need for adequate navigation systems.

API (Applications Programme Interface) is an operating system comparable to e.g. Microsoft Windows in the computer world. It controls the functioning of the set-top box and defines the software interface the digital programme application needs to find in that box in order to be able to run the programme. In this, the API has an important function for the compatibility of interactive software necessary to operate certain services and the set-top box.

An EPG (Electronic Programme Guide) is navigation software for digital TV, for example the equivalent of a Web browser. It leads the consumer through the increased offer and enables him/her to access information on all available services.

Often APIs and EPGs are designed and licensed by vertically integrated actors, which typically also control proprietary CA systems, programming rights and subscriber management systems.[41] The controller of an API can prevent a programme reaching the consumer in several ways, by e.g. designing an API that it is unable to support certain services, refusing to provide access to the technical specifications necessary to interact with the API, or providing access on disadvantageous terms.

The ergonomics and presentation of the EPG will be an important element of competition between bouquet providers. A particular operator's EPG may not recognise another broadcaster's EPG, and therefore only identify its own channels and not those of third parties. Control of an EPG provides the opportunity to influence viewing shares and to take strategic control of the market, as it is the service that informs viewers about available services.[42]

As a result, APIs and EPGs will play an important role not only in the management of the expected growth in the number of channels, but also in the relation between pay and free CA services and their availability for consumers.

So far, the Standard Directive has not dealt with the issue of fair access to EPGs and APIs, and Member States have dealt with it only marginally. In this context, Italy and Ireland[43] should be mentioned, as they are two of the few countries to have drafted legislation that adopts provisions on the fair operation of EPGs and APIs. Also in the UK, issues of interoperability and fair competition have been dealt with quite intensively, e.g. by ITC[44] and OFTEL. Further initiatives are undertaken by state-independent institutions on the basis of self-regulation (e.g. the DVB Group, the FUN Project in Germany, etc). Initiatives, however, still focus primarily on the pay-TV sector.

For IS services the situation is different. While also IS service providers use conditional access systems for non-remuneration reasons, there will be probably generally no bottleneck facility involved. Conditional access is a bilateral agreement between the service provider and the user. Open standards are used to enable these conditional access solutions. There are no obvious differences between the use of conditional access for remuneration reasons and the use for non-remuneration reasons.

A further question is, whether additional legal protection of CA systems for non-remuneration reasons will foster market development for additional services and/or for CA devices. The experience gained with the CAD protecting CA use for remuneration reasons seems to suggest that this might be the case. However, the initial situation is different now from what it was a few years ago. First of all, CA systems are already used for non-remuneration reasons by those broadcasters who can derive a sufficiently high utility from doing so. A few years ago pay TV was still in its infancy. Identifying the surge in pay TV as caused by the CAD might be a *post hoc ergo propter hoc* fallacy.

---

[41] See Chris Marsden, 'Pluralism in the multi-channel market: Suggestions for regulatory scrutiny', study for the Council of Europe, MM-S-PL (99) def., Strasbourg, 11 October 1999, Section 4.2.
[42] C. Marsden, Section 4.2.
[43] Annex I, sections 2.1.8 and 2.1.9.
[44] ITC Code of Conduct for Electronic Programme Guides, October 1997, www.itc.org.uk/regulatory/eco-reg/epg.htm .

Secondly, even if there is an increasing demand for CA systems, the broadcasters would most likely use already existing systems instead of developing new ones. In most cases, the use of existing systems would be cheaper due to advantages of mass production. This is especially important for the use of CA systems for non-remuneration reasons, as the costs cannot easily be passed on to the customers.

If there is, however, an increase in CA use for non-remuneration reasons this will most likely reduce the price of existing devices instead of increasing the number of choices. The real consequences might follow from the price fall. It might induce even more operators to use CA devices, as the total cost of employing CA solutions falls. This in turn might eventually increase the number of programs, as it also decreases the CA cost for service providers.

For information society service, however, the consequences of additional protection are probably even smaller, as CA systems are in frequent use also for non-remuneration reasons. Providers have typically chosen a technical rather than legal protection of their service, as already set out above. Thus, it is questionable if additional legal protection will have significant positive consequences.

3.3. Impact on technical progress

With respect to the impact of a CAD extension on technical progress, two different issues must be distinguished. The first are potential consequences for the development of the markets for CA devices. The second impact comes from unintended consequences on other market and was already subject to discussion at the time the CAD was drafted but also in context to the recent preparations for a draft Copyright Directive.

It has already been set out above, that the direct consequences of an increase in legal CA protection eventually will not lead to a significant technological advancement in CA devices. First of all, potential new users of CA systems can already choose from a variety of systems, so that the necessity to develop new ones is relatively small. And secondly, additional legal protection reduces the necessity to improve the encryption technology embedded in the CA systems. Thus, the positive effects on technical progress due to additional legal protection of CA use for non-remuneration reasons will most likely not be very large.

Whether there are unintended consequences for other markets to be expected, depends very much on the exact wording of a CA extension. According to the CAD, illicit devices are “any equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorisation of the service provider”.

If an extension declares all software and devices illegal that are suitable for circumventing CA systems, then the potential impact can be very strong, as also legitimate products like general-purpose PCs and software can fall under this definition. In this case it is to be expected that technical progress can be seriously hindered. This also includes the development of new and better forms of encryption, which could also be used to improve CA systems.

In the IS service domain the consequences could be even more severe, as the distinction between technology used to enable CA solutions and technology used for other purposes is rather fuzzy. After all, in most cases general-purpose software is used for conditional access systems, whereas in broadcasting CA systems are generally special hardware devices or some

combination of hardware and software. Thus the chance that general-purpose technologies are banned from an extension of the CA Directive is rather large.

Considerations of this kind where grounds for recent proposals in the frame of the preparatory works on Article 6 of the draft Copyright Directive,[45] which probably will restrict the notion of illicit devices to such devices "which have only a limited commercially significant purpose or use other than to circumvent or are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating" a circumvention. Similarly, the analysis of existing national legislation has shown that some national legislators (e.g. in Japan and the US)[46] chose to concentrate prohibitions on devices that are *primarily designed or produced for the purpose of circumventing*. Other countries (e.g. Finland) provided for the possibility to grant, in exceptional situations, permission to use certain circumventing devices.

The underlying idea is that general-purpose electronic equipment and services should not be outlawed merely because they may *also* be used to circumvent protected measures or services.[47]

Most severe might be the consequences for scientific and technical progress in cryptography. Currently there exists a strong open competition between creators of cryptographic solutions and pirates who try to crack them. In some circumstances even the creators of solutions conduct contests for hackers to find out whether the new solution is really as tamper-proof as expected, or whether it can be hacked. If parts of this activity are coincidentally declared illegal, the scientific progress in cryptography might be slowed down.

All in all, a broad extension of the CAD possibly would have negative consequences on technical progress. If the CAD shall be extended, one would have to take care of keeping up scientific and technical progress in this area.

3.4. Impact on consumer welfare and choice

The impact on consumer welfare and choice of extending the CAD to services provided not for remuneration depends very much upon the impact on market structure and competition on the one hand and the impact on technical progress on the other hand. If competition decreases – perhaps because pay TV broadcasters will be exposed to reduced competition from services which can be received without set-top boxes – prices tend to rise which decreases consumer welfare. On the other hand an increased demand for set-top boxes will probably reduce their prices. This not only benefits the consumers of an increased offer of new services but also enables already existing pay TV operators to lower their subscription fees. Thus, the final outcome is uncertain and even an estimation of its sign would be purely speculative. A serious estimation would require the analysis of cost structures of broadcasters, their strategies as well as alternative technological development trajectories, which goes far beyond the analysis conducted here.

[45] Annex I, section 1.2.4.
[46] Annex I, sections 2.2.3. and 2.2.4.
[47] See amended draft Proposal, Recital 20bis, Annex I, section 1.2.4. : "... without, however, preventing the normal operation of electronic equipment and its technological development; ... whereas such legal protection should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection; whereas, in particular, this protection should not hinder research into cryptography".

A second potential impact on consumer welfare can result from the impact an extension of the CAD can have on technical progress. However, just as can be seen from the example of strong US export regulations for encryption software, other countries with more liberal regulations will gain a competitive advantage. In any case, if technical progress is slowed down, consumers forgo new products and services they would otherwise be able to purchase. Thus, consumer welfare also decreases.

Also in relation to consumers, bottleneck aspects of CA devices or components thereof may be of relevance, particularly the issue of EPGs and APIs deserves to be mentioned. Both these components of a CA system can be used to control how e.g. digital television reaches the consumer, and thus to manipulate choice. As the audience becomes increasingly fragmented across multiple channels, the navigation software (EPG) will become the crucial tool for influencing viewing patterns.[48]

Similarly, APIs will be used to determine whether certain services or programmes can be operated on the viewer's set-top box. Similar problems may arise in the field of IS services as regards the issue of the fair use of Web browsers and the interoperability of the necessary operating systems.

The interoperability of and preventing the abuse of such systems may be thus of fundamental concern for the access of consumers to CA broadcasting services. The user must be able to switch between competing providers without incurring additional costs. To be able to do this, the consumer needs additional information and guidance. Otherwise, as stated by concerned parties, there may be the danger of extreme channel subscription increase by consumers who are locked into a particular CA system. In this context, the Italian initiative[49] should be mentioned: it proposes to oblige operators of CA devices and EPGs not only to grant service providers free access to systems, but also to inform consumers in an appropriate way on all (including competing) existing services.

However, there is also the matter of choice but also the general availability of contents to consumers as such, irrespective of the question of technical bottlenecks. Control of access to services means that access to certain services or contents is made conditional on certain requirements; in other words, it is no longer 'free' (in the sense of unconditional).

The potential impact of extending the CAD on consumers' choice is also a quite complicated issue. The quite obvious part is that the number of freely receivable broadcasting channels decreases if broadcasters decide to employ CA systems where this has formerly not been the case.

Naturally, this is a point where consumer organisations and other parties are particularly concerned. It was argued that any legal protection afforded by national legislators to free CA service providers would be an infringement of the rights of citizens to receive information and ideas without government interference, as protected e.g. under Article 10 ECHR, unless it could be shown that the protection is both prescribed by law and necessary in a democratic society. Otherwise, any legislation forbidding technical systems that seek to bypass CA systems that are used by providers of free CA services would run counter to those rights.

[48] Marsden, ibid, section 4.3.
[49] Annex I, section 2.1.9.

Article 10 ECHR grants citizens the right to receive and impart information regardless of frontiers, and that any restrictions of this right must be based on due considerations of other legitimate interests deriving from legal protection.

However, it is questionable whether the mere granting of legal protection against piracy activities means a restriction of the right of consumers to receive information.[50] One must bear in mind that even where service providers use such devices, they are naturally interested in being received by consumers. Secondly, as mentioned, the use of CA by free CA services could possibly also have positive effects in the case of a multiplied offer of services and choice. Furthermore, as the Council of Europe has argued, the right of citizens to receive information does not provide a right to override legitimate interests (i.e. access to information does not necessarily imply a right of unconditioned access) as long as the conditions are justified by the adequate interests of service providers.[51] The use of access control is, consequently, also a matter of balancing interests. In other words, as far as service providers have valid (mostly economic) reasons to use CA, these may eventually justify their application.

The question is, first of all, whether there may be situations where the interests of consumers to receive services or information must be regarded of higher value than the interests of a CA service provider to use CA.

Canada, for example, recognised such an interest where a service provider had obtained the legal rights to provide a programme for a certain area, but failed to do so.[52] In this case, particularly where a broadcaster prevents other services from being licensed for this area, the Canadian legislator has recognised a protection-worthy interest of consumers to access the service, even without authorisation from that service provider.

The interest of the general availability of certain information was also subject to Article 3a Television Without Frontiers Directive:[53] "Broadcasters shall not broadcast on an exclusive basis events which are regarded as being of major importance for society in such a way as to deprive a substantial proportion of the public of the possibility of following such events on free television." This was to guarantee public access to national or non-national events of major importance to society, such as the Olympic Games, the (football) World Cup and the European (football) Championship, and to give Member States the possibility to draft so-called lists of important events which they wish to see remaining on free TV.

Apart from the question whether providing consumers with major sport events already fulfils the interest and need of consumers for information, it is also questionable what the position of the Television Without Frontiers Directive towards encrypted free CA services is. As can be concluded from the Directive ("free television means broadcasting on a channel, either public or commercial, of programmes which are accessible to the public without payment in addition to the modes of funding of broadcasting that are widely prevailing in each member state (such as a licence fee and/or basic tier subscription fee to a cable network"), free CA services are considered any services which do not require additional payment; in other words, Article 3a of the Directive probably aims at exclusive rights for pay-TV providers only, whereas also free CA service providers are in a position to exclude major parts of the public from such

[50] See also Article 10 Section 2 ECHR.
[51] Council of Europe, Recommendation 91(14), Explanatory Memorandum, Note No. 8.
[52] Annex I, section 2.2.2.
[53] Annex I, section 1.2.6.

events. Furthermore, the Television Without Frontiers Directive does not deal with free access to contents on the Internet.

The second question is whether access control of services necessarily means to restrict the general access to them.

Indeed, as examples in Denmark, Sweden, the UK (and soon Austria) and other countries show, the use of CA systems by free broadcasters does not necessarily mean excluding the public from access to programmes. Decoding equipment can be distributed to the population free of charge or against modest compensation, in order to enable, in principle, the whole population to receive public broadcasts. It is another question whether the whole population would actually be able to receive programmes, bearing in mind that the implementation and operation of decoding equipment requires a certain level of technical skill, which may prevent e.g. older people or children from gaining access.

Surprisingly, at the moment it is primarily public broadcasters which are showing ambitions to implement CA devices for non-remuneration reasons and drive the development—apparently mostly for copyright reasons, but also with a view to the possible enhancement of their service/digital service offers. Traditionally, public broadcasters are considered to play a particularly important role in the realisation of citizens' information rights; e.g. Article 10 ECHR: "considering that the system of public broadcasters in the Member States is directly related to the democratic, social and cultural needs of each society and to the need to preserve media pluralism...".[54] To a certain degree, they are treated as a guarantee that the public will be provided with a certain amount of necessary information.

Less surprisingly, the question of whether access control sits comfortably with the public mission of public broadcasting is still subject to very controversial discussions within Member States. Whereas in some states, such as Germany, the dominant opinion is that the public mission of broadcasting forbids the implementation of CA devices in relation to consumers, apparently not all Member States share this opinion.

However, if keys are distributed free of charge to the legitimate receivers – as has been the case e.g. in Denmark – then consumers should be equally well of as before. The main question remains what happens to those who are not the broadcasters' target population but were able to receive the channels before, e.g., Danish expatriates in France.

The use of CA devices for non-remuneration reasons may mean that audiences living in other countries are excluded from access to services. This again may have an impact on the rights of consumers as granted under Article 10 ECHR, which explicitly grants the right to receive information *regardless of national frontiers*. Particularly where (up till now) free national broadcasters use CA devices to restrict the transmission to a national or language territory (e.g. due to obligations deriving from copyright licenses), this may bring with it the danger of a fragmentation of the European broadcasting landscape into various country or language zones.

Territorial fragmentation may have an impact on the accessibility of programmes to citizens of one country who have moved to another country. Where the decoding of, or preparatory activities for decoding, free CA services was prohibited, a decoder legally obtained in one member state could be illegal when brought into another member state. The Danish citizen

[54] See Protocol 32, Consolidated version of the Treaty establishing the European Community, Amsterdam, 16-17 June 1997.

living in France, for example, may thus be prevented from accessing the encrypted broadcasts of DR1 and 2, and thereby from accessing his/her cultural heritage.

However, the opposite example may be a channel operated by YLE called TV Finland, an encrypted satellite channel which is distributed over Europe for expatriate Finns. The channel is an edited channel consisting of programmes picked from YLE TV1, YLE TV2 and the commercial channel MTV3 Channel. The programmes are retransmitted simultaneously and unchanged.

The control of access to national services may also have a direct impact on the diversity and plurality of the international programming available in Europe. The example of Luxembourg may explain this: Luxembourg has almost no own programme services; currently, there is one national service in Luxembourg which transmits programmes for approximately one hour a day. Luxembourg's supply of broadcast programmes therefore depends almost entirely on services from neighbouring countries, which are, thanks to spill-over effects or transmission agreements, also accessible in Luxembourg. Where neighbour countries decide to encrypt their national services (e.g. for copyright reasons) and to provide the necessary decryption devices only to their own citizens, their programmes would no longer be receivable in Luxembourg. Also, broadcasters from neighbouring countries will probably not always purchase the additional licensing rights for Luxembourg in order to make their service available also in that country.

On the other hand, CA techniques may enable the future licensing of rights on the basis of the actual number of users rather than according to national frontiers. Furthermore, with the increasing use of the Internet as means of distribution of services or contents it becomes questionable whether the current licensing practise on territorial basis will be maintained.

Other problems concerning general access to contents emerge from the relation of pay and free channels and the praxis of bundling digital broadcasting channels. Multiple channels allow vertically integrated operation to acquire a monopoly of programming, which can be bundled in a bouquet of channels and sold through a proprietary CA system.

As one effect of bundling, consumers can be urged to buy the whole package. A more serious implication, however, may be the possible difficulties consumers encounter in accessing the free CA services included in such a bundle, e.g. public broadcasting services. As mentioned, in the UK for example, SkyDigital and On-Digital are already bundling free CA services, such as BBC1, BBC2, ITV, and Channels 4 and 5. Another example is the digital programme bouquet of Canal+ in the Netherlands, which also includes free broadcasters. Operators of digital multichannel bouquets are in a position to exclude consumers who have not subscribed to their service from accessing the services in their bundle, even if the free CA services in that bundle are only encrypted for security reasons. Against this background can be understood, for example, the US regulation[55] which provides that public broadcasting services may not be encrypted unless it is guaranteed that they can also be received in unencrypted form.

Service operators could also exclude other, less popular programmes from their offer. Consumers who have subscribed to their service would then have to choose between not watching these programmes or additionally subscribing to another system—a praxis which may influence consumer's choice as well as the plurality of offers.[56]

[55] Annex I, section 2.2.4.

[56] See also Committee on Legal Affairs and Citizen's Rights, Report on the proposal for a European Parliament and Council Directive on the legal protection of services based on, or consisting of, conditional access,

Some Member States have already taken the initiative with respect to channel-bundling (e.g. OFTEL in the UK). The OFTEL regulations, however, e.g. only apply to bundles offered to cable operators, not those offered directly to the consumer.

It should be noted that digital multichannel services include, besides broadcasting services, other services, e.g. interactive services (home banking) or IS services, such as Internet access, etc. Consequently, the same argument about the exclusion of third parties can be made in relation to the online shopping services operators include in their bundle.

Although issues of access to information have been dealt with in the past mostly in the context of broadcasting services, the time may have come to acknowledge the growing importance and role of e.g. online services in providing the public with information and assisting the public opinion-making process.

Up to now, we have focused on questions of a possible impact on the general accessibility of contents. Not so obvious is the impact of a CAD extension on the number of CA protected channels and the question of increased offer and choice. First of all there is the question, whether the Directive can induce free TV broadcasters to offer more, possibly more specialised channels. This could be the case if license payments for copyright-protected material are so high that programs based on this material up to now have not been economically feasible. At the same time, the willingness to pay for such program must be so low that they are not yet offered by pay TV broadcasters. It is rather difficult to think of examples where this might be the case.

A second question is whether an increased use of CA systems for non-remuneration reasons will have any indirect consequences on the number of channels. There does exist one such connection that might be important. If prices of CA equipment decrease due to higher demand, pay TV operators can lower their fee and thereby increase their user base. This, in turn, might increase the number of special-interest users sufficiently to make additional programs profitable and thereby increase diversity. However, whether this will really be the case depends very much on the reaction of broadcasters to changes in the legal system, the price changes upon additional demand, the reaction of pay TV producers and finally the number of additional pay TV users this generates.

For IS service providers as opposed to broadcasters it has already been argued above that the potential impact on market structure and competition by an extension of the CAD will probably be rather small, as already most service and content providers who are interested in using CA systems do so. As a consequence there is also no significant impact on consumer choice to expect.

When discussing the interrelation of the use of CA devices by free CA services and access to information, perhaps the question is less whether it is generally desirable for also free service providers to use or use not CA devices, but under which conditions free service providers finally make their services accessible.

COM(97)0356, 21 April 1998. Amendment 16 proposed to introduce a provision stating that the right of viewers to have access to free-to-air channels within a conditional access service platform without being required to pay an additional fee beyond the normal charge for accessing the platform.

In case of pay-TV, the situation is still relatively transparent: service providers use CA devices in order to make access conditional on the payment of a fee. As long as this fee is not unreasonable large (a large fee would mean that access by the less favoured sections of society would be rendered difficult) and there are still 'free' alternatives, the danger of a possible abuse is relatively small.

The situation may be different, however, where CA devices are used by free service providers: the condition for gaining access is no longer simply the payment of a fee. Access can be freely determined by the service provider, since electronic access control allows the provider to determine who may access a service and under which conditions.

Particularly in the field of IS services (e.g. one-to-one services and certain e-commerce applications), CA devices allow the service provider to individually identify and choose to whom services are transmitted or—the other way round—whom to exclude from access. Considering the growing importance of the Internet for the process of gathering information, this may raise some concerns about basic consumer rights (such as the right to information and non-discriminatory treatment) if the service provider's decision is unfair and/or discriminatory.

But even where the criteria according to which service providers decide to whom to grant access are not per se unfair and/or discriminatory, the very criteria used in a particular situation may conflict with consumers' rights. Service providers have agreed that to some extent CA techniques could be used to acquire better knowledge of and control over the behaviour of each consumer of services.

Examples can be found in e.g. the field of e-commerce. Here, CA can be used to require consumers to fulfil certain obligations or requirements established by the service provider before they are granted access. For example, when subscribing to an free online service, a bulletin board, etc., a service provider may present the consumer with a list of terms and conditions drawn up by the service provider (so-called caller contracts or acceptable user policy; AUP). AUPs can include information on what will happen to data the consumer submits, the copyright consequences of distributing a text, liability limitations, etc. The consumer will be required to take notice of these conditions, and the service provider, by means of access control, can hinder the progress of the access process until the consumer has accepted the conditions or complied with other conditions of the operator, such as providing certain personal information or prior identification. In other words, a service provider can use CA devices to make the user comply with the conditions of the service provider, whereas the conditions are not necessarily always in the interests of the consumer or give him/her the possibility to influence those conditions.

Where CA devices are used by providers of free CA services to identify consumers and gather information on them, this may also have impacts on consumer's privacy and the protection of personal data. This is already a concern in the field of pay CA services. It is even more so where service providers implement CA devices *primarily* for the purpose of gathering information. For example, providers of online services make access to their service conditional on the provision of certain personal information concerning the consumer and his/her online behaviour, profession, marital status, sex, hobbies, preferences, number of hours spent online per week, etc. A more subtle method, based on a technology called GUID (Globally Unique Identifier), can be used together with CA techniques to identify and classify each user of a website. By using CA devices, a service provider can persuade consumers to

reveal personal information, since this—in the view of the average consumer—is the only way to gain access to the 'free' service. In some cases, the user will have no idea what will happen to this information, whereas it may represent for the service provider considerable economic values.

It is questionable to what extent existing national laws on data protection provide for the sufficient protection of consumers in such situations. Interestingly, the American DMCA provides for one exception: it seems to give to users a right to 'self-defence' by allowing circumvention of CA devices where such are primarily used to collect information on consumers' online behaviour.[57]

But identification on the basis of consumer information may also raise concerns regarding consumer's privacy, for example the consumer's interest to remain anonymous. In the offline world, we would probably regard it a serious intrusion into our private sphere if a shop assistant were to start asking us questions about our shopping behaviour, favourite vegetables, number of children, preferences and time of hours per week spent in local shops, etc. The intrusion would be even worse if answering those questions was a precondition for being served and for purchasing goods.

Other possible conflicts where CA devices are used to protect not services but works in this sense of copyright law are not subject to this study and therefor shall be mentioned only shortly.[58] By preventing access to works, service providers can simultaneously prevent acts of authorised exploitation of such works. This is why e.g. Australia and the US (in the DMCA),[59] but also Article 6 of the Draft Copyright Directive,[60] try to find a balance between the interests of rightholders (and, indirectly, service providers) to use technological measures to protect works, and possible consumer interests to use such works where this is allowed by law.[61]

3.5. Conclusions

The use of CA devices for non-remuneration reasons is still in its beginning. Therefor, it is too early to give a serious prognosis on the impact of CA use on the Internal Market and its market players, particular competitors and consumers. Furthermore, the use, development and impact of CA is part of a broader and more complex problem which goes far beyond the scope of this study. Therefore, further research is needed to assess possible implications and consequences of an increased CA use, but also of a possible extension of the CAD.

As experiences in the pay-TV sector have already shown, however, one factor which probably influences market structure and competition on broadcasting is determined by the bottleneck character of CA systems. This is particularly true for the broadcasting sector, whereas in the IS service domain, less bottleneck problems seem to exist.

[57] Annex I, section 2.2.4.
[58] Extensively, see Kamiel Koelmann, 'A Hard Nut to Crack: The Protection of Technological Measures' , European Intellectual Property Review 2000, p. 272-288.
[59] Annex I, sections 2.2.1. and 2.2.4.
[60] Annex I, section 1.2.4.
[61] See also chapter 5.2.11.

An increased CA use also could have implications for consumers' interests, particularly consumer's access to services which were previously free, the involvement of public broadcasting in the CA use, the possibility to influence the behaviour of consumer's by means of CA use, but also the impact of increased CA use on general choice of services offered. On the other hand, a rise in CA use for non-remuneration reasons will most likely decrease prices of CA. This possibly could encourage e.g. TV operators to offer additional niche services.

Whether an extension of the CAD finally would increase the use of CA for non-remuneration reasons is not entirely clear. Even if the CA use would rise, modifications and use of already existing CA systems are more likely than the development of new systems. Whereas the impact of an extension of the CAD on technical progress of CA systems in general will depend on the strength of protection offered.

4. Problems with and related to piracy

4.1. Piracy of conditional access devices used

Piracy of services is a very sensitive issue. Consequently, the availability of relevant data is rather limited. Many providers of free CA services claim that they have had no experiences with piracy as yet. We have already mentioned, though, that the use of CA techniques by providers of free CA services is still in its infancy; it is thus not too surprising that not much experience exists with the piracy of such services. Secondly, the piracy of a provider's own devices is still hardly admissible in such a competitive environment. They are therefore reluctant to state whether or not their systems have been pirated. Moreover, since CA devices can serve many purposes simultaneously, it is not always possible to determine what purposes a pirate device is supposed to serve.

On the other hand, the range of pirate devices available shows that a market for equipment to view free controlled-access services certainly already exists. For example, a large amount of such decoding equipment or services can be found offered on pirate sites on the Internet.

The experiences of providers of pay-TV services have proven that the use of CA devices can be hindered by considerable piracy problems.

According to AEPOC (Association Européene de Protection des Oeuvres Cryptées), the level of piracy in Europe at the end of 1996 represented more than ECU 200 million in revenue lost annually by European pay-TV broadcasters, rightholders and other content providers. A study to assess the evolution of this figure up to 1999 is currently being conducted.

It remains to be seen how far the providers of services using CA devices for non-remuneration purposes are also exposed to piracy activities. In this context, also the general technological progress of CA devices and their improving security may play a role. Due to the lack of available relevant data, at the moment there is room only for speculation.

However, it must be borne in mind that even where CA devices are used for non-remuneration purposes, this will be done (as far as the scope of this study is concerned) in an economic environment and mostly in order to protect economic value and content.

Services examined contain valuable content (such as copyright-protected and other programme material, information, data, etc.), although not provided in return for direct remuneration. Apart from the value of the content, the service itself may also have considerable economic value – for example, where broadcasters use CA devices in order to prevent the unauthorised retransmission and commercial exploitation of their programmes by pirates. The recent discussions on the need to implement legal protection of technological measures, in the field of copyright[62] for example, shows that a threat of piracy certainly also exists when no direct remunerative interests are at stake.

Cases have been also reported of the purchase of circumventing devices in order to overcome territorial restrictions. In Australia, for example, the transmission of certain local football

[62] Annex I, section 1.1.4.

matches was restricted (due to the underlying licence agreements) exclusively to the area in which they were played. Nevertheless, pirates developed smart cards which enabled the inhabitants of other areas to receive the transmissions.

Other possible motives for circumventing free CA services feared by providers include unauthorised access to services intended for another target group (e.g. medical data services), and (marketable) interests in circumventing legal restrictions, e.g. with regard to the protection of minors, data protection, secrecy of communication, etc. Here, additionally, the interests of service providers and of third parties in protecting sensitive information may be involved.

Consequently, providers of free CA services have expressed their concern about the possibility of being hacked in the future – even if they may have not (yet) experienced any piracy.

Free-service providers also claim that sometimes the same CA techniques are used by providers of both free and pay services (e.g. in case of satellite transmission). In this case, once a system is hacked all services protected by it - free or paid-for - are exposed to pirate activities to the same extent - although, under the present CAD, providers of free CA services cannot claim any legal protection against the piracy of devices which are used for non-remuneration purposes.

But providers of pay-services also show some concern and doubt as to whether the CAD in its present form provides efficient protection. As indicated above:

a) CA techniques can serve remunerative and non-remuneration purposes simultaneously; and
b) in some cases the same device is used to protect free as well as pay services.

Under the present wording of the Directive, pirates are in a position to claim that their activities are limited to providing access to free CA services. This argument has been used, for example, in Italy, where the pirates asserted that their decoding devices were not intended to provide unauthorised access to Tele+ but to a free foreign channel which had been encrypted for copyright reasons.[63] The defendants affirmed that their devices were programmed with the purpose of decoding the encrypted foreign channel which was airing its analogue signal by satellite using the same system as Tele+. According to the pirate organisation, it was mere coincidence that Tele+ could be decoded using its device. Unfortunately, the case was not resolved since the Judge for Preliminary Inquiries decided not to proceed against the company since – in his opinion – the charge was (for other procedural reasons) groundless.

A similar case reported from Germany concerned multifunctional decoders which are also capable of circumventing non-remuneration services.[64] During the proceedings, the defendant claimed that his devices were multifunctional and not specifically designed to circumvent the CA devices of the plaintiff. The defendant had been selling devices which could be used for a variety of purposes, including to gain access to the CA-based pay service of the plaintiff. But he claimed that his decoders were not specifically designed to enable unauthorised access to that service. However, the court did not accept this argument and convicted the defendant of an offence under Article 1 of the German Unfair Competition Law (Gesetz des unerlaubten Wettbewerbs – UWG).

[63] Annex I, section 2.1.9.
[64] Annex I, section 2.1.6.

Similar difficulties may arise in a situation where free CA services are provided together with premium pay-TV channels in a digital programme package, but no payment is required to access the free channels. Although the free CA services will be encrypted, no remunerative interests are involved. Again, pirates may claim - where national law focuses upon the protection of directly remunerated programmes - that their device was intended not to circumvent any remunerative interests but to provide access to the free CA services in the package.

Finally, when decoding devices can be used for several reasons simultaneously (as is usually the case), pirates could claim that their devices are not designed to circumvent the potential remunerative interests of service providers but to collect information or personal data, or to overcome geographical restrictions.

In all these situations, efficient protection depends upon the individual judgement of courts and how national judges deal with arguments as described above. Where there is any doubt, it is probably up to the service provider to prove that the illicit devices were designed to circumvent remunerative interests.

There was also some concern that not prohibiting the manufacture of devices designed to circumvent CA for non-remuneration purposes may encourage the development of the general pirate market.

Summarising, there is no actual evidence for a piracy problem of decoders which are used for non-remuneration reasons. There are, however, some clear indications that it is likely, that providers of free service are exposed to pirate activities, whereas the distinction between remuneration and non-remuneration reasons to use CA under the CAD may fail even to effectively protect providers of pay CA services.

4.2. Forms of pirate activities

Due to a lack of available information, it is not clear yet what forms of piracy free-service providers may experience. There are no reasons, however, to assume that they would differ considerably from the unlawful activities to which providers of pay CA services are exposed. These are both individual acts of unauthorised circumvention and preparatory activities as already addressed by the CAD (manufacture, import, distribution, possession for commercial purposes, etc.).

Other possible forms of piracy mentioned by service providers are the use of illicit devices for the unauthorised retransmission of services for commercial purposes, the manipulation or modification of legal devices to decode, and the sale and other forms of distribution (i.e. free) via the Internet of information and services needed to circumvent CA systems.

4.3. Consequences of pirate activities

Again, the lack of relevant data makes it impossible to make any firm statements. However, when asked for possible consequences of piracy for their services, providers of free CA services approached expected that the consequences of piracy would be similar to those

already experienced by providers of pay services. Particular fears were loss of confidence by content providers and legal repercussions due to the breach of statutory contractual obligations. Loss of confidence by content providers in the security of free CA services could have severe economic consequences for service providers, for example where content providers are unwilling to licence contents to providers of free CA services if the distribution of content does not seem to be sufficiently secure. This again could considerably weaken the negotiating position of providers of non-directly remunerated services. Other possible consequences listed were the time and money required to replace pirated systems (which is, by the way, probably a particular problem in the broadcasting sector), as well as possible financial injury to third parties. Whereas the loss of subscription fees or subscribers naturally is not a concern for free service providers.

4.4. Cross-border aspects of piracy

Only a few operators of free CA services were able to answer questions on the efficiency and enforceability of existing legal protection, as well as on the impact of the absence of such regulations on their national or international activities.

Other operators, however, indicated that due to the absence or to different levels of protection in other countries, law enforcement in their own country was difficult - either because the national police force lacked the competence to stop illegal activities outside the home country or because infringing activities were not unlawful in the originating foreign country.

The experiences of providers of pay-TV services have shown that cross-border piracy constitutes a serious problem, particularly where national legislation is unharmonised and offers different levels and scopes of protection.

Examples are:
- the transfer of valid decoding equipment from the legal owner in one country to an unauthorised owner in another
- the "cloning" of pirate cards in countries for which a broadcaster has not licensed any transmission rights, particularly where the country offers no protection to foreign programmes (whereas the federal legislation of the US covers both interstate and foreign services)
- the manufacture, distribution, sale, etc., of decoding devices in states where no adequate protection exists
- making available or publishing necessary information or passwords, or distributing decoding software over the Internet and
- flaws in the field of law enforcement between the Member States, such as a lack of co-operation, knowledge of foreign legislation etc.

The position of free-service providers is even more difficult, since less specific protection exists and unauthorised activities against them are prohibited only in a small number of Member States.[65] This is even more true for providers of free CA information-society services. As a consequence of their largely ubiquitous character, they are even more open to piracy from “safe-haven” countries.

[65] Chapter 5.2.

It was also argued that distinctions within national laws between situations in which CA devices are used for remunerative or non-remuneration purposes would increase legal uncertainty and make room for the circumvention of such regulations.

When asked about the consequences for their marketing and security policy of the removing the disparities between the legal protection offered in different states, providers of both free and remunerative CA services stated that in the first place they would seek to increase the efficiency of CA techniques. Contractual solutions have been tried, but proven rather difficult to effectively establish and implement.

In general, providers of CA systems are continuously working to improve system security. This includes the constant probing and analysing of pirate technology, incorporating security upgrades and devising anti-piracy strategies for service providers. However, substantive costs could be involved which may be disadvantageous for smaller service providers with smaller resources which have, consequently, less potential to defend themselves against piracy.

4.5. Conclusions

It is as yet unclear to what extent providers of free CA services will be exposed to piracy and what consequences this, and the scope of protection under existing national legislation, will have upon their activities. The same applies to the question as to what extent the provision of national and international services will be hampered by acts of cross-border piracy, and whether existing specific and general laws are effective to fight the consequences. The level of experience and data available is still to low to allow any firm assessments.

There is, however, little reason to assume that providers of free CA services will be considerably less concerned by pirate activities than providers of pay services – particularly when those services consist of the transmission of economically valuable material and are provided in an economic environment.

The consequences of the piracy of services using CA devices for non-remuneration purposes may at first glance be appear less serious than is the case for pay-TV providers, since circumvention would not directly threaten the service's source of financing. Providers of such services would, however, have to fear considerable competitive disadvantages in respect of the content industry, and the loss of time and money required to replace pirated systems. Secondly, also with free CA services, CA devices are generally used to protect economically valuable material. It also has to be borne in mind that providers of non-remuneration services, particularly smaller operators, may find it more difficult to raise the money necessary to compensate losses since they depend upon indirect methods of financing.

Adverse effects may also, as the experiences in the pay-TV sector already have shown, imply negative consequences for the interests of third parties such as rightholders, other content providers and the producers of CA devices for non-remuneration purposes.

5. Legal protection of conditional access services

5.1. International regulations

5.1.1. Introduction

A few international regulations on the level of EC, WIPO and the Council of Europe deal with the legal protection of technological measures.

In the following, we will introduce these regulations and examine to what extent they may be of interest for the protection of providers of non-directly remunerated CA services.

5.1.2. Council of Europe

In 1991, the Council of Europe adopted Recommendation 91(14) on the legal protection of encrypted television services. As the name suggests, the Recommendation aims at the protection of encrypted television services; radio broadcasting and IS services do not fall under its scope. The Recommendation suggests that Member States should prohibit certain preparatory activities in order to combat commercial activities with unauthorised decoding equipment, and to provide effective penal or administrative sanctions as well as civil remedies. Unlike the CAD, the Recommendation does not make protection conditional on whether encryption techniques are used by providers of free or of pay services. Although it recognises the particular meaning of encryption for pay-TV, it acknowledges that the technology may also serve other reasons than to ensure remuneration interests. [66]

The Recommendation inspired several Member States of the Council (e.g. Denmark, Finland, France, Ireland, Switzerland and the UK) to adopt specific legislation on the legal protection of CA services, although only some of these countries decided also to protect non-directly remunerated CA services.

The proposed CA Convention of the Council of Europe follows the model of the CAD and protects CA devices only in so far as they are used by providers of pay-TV and IS pay services. Furthermore, the Convention expressly states that reasons to use CA devices other than to ensure remuneration interests are not covered, but could be dealt with better in a separate instrument; in this context, it referred to existing or proposed regulations at the level of WIPO or the EC in the field of copyright.

5.1.3. WIPO

[66] Note, the Committee of Experts on Crime in Cyber-Space (PC-CY) of the Council of Europe is currently preparing a Draft Convention on Cyber-crime (Draft No. 19). The Convention, once it has been adopted, may add to the protection of computer systems (in the sense of any device or a group of inter-connected devices, which is based on the function of data processing, including telecom systems, Articles 1 (a), 2 of the Draft Convention) against unauthorised access. Since the present study focuses in the main place on content-based broadcasting and IS services, however, the draft Convention will be not discussed here more detailed.

At the level of WIPO, in 1996 the Diplomatic Conference adopted two treaties—the WIPO Copyright Treaty (WCT) and the WIPO Performers and Phonogram Producers Treaty (WPPT)—both of which require contracting parties to provide adequate legal protection and effective legal remedies against the "circumvention of effective technological measures that are used by authors (WPPT: performers, phonogram producers) in connection with the exercise of their rights under this Treaty … and that restrict acts, in respect of their works, which are not authorised by the authors concerned or permitted by law". In doing so, the Treaties deal with a specific non-remuneration reason to use CA (i.e. the protection of intellectual property rights), but are only of limited interest to service providers since the treaties address rightholders, performers and phonogram producers, not broadcasters or providers of IS services.

The WIPO Standing Committee on Copyrights and Neighbouring Rights is currently discussing a new initiative in the field of neighbouring rights with a view to the protection of broadcasting organisations. In this context, it is planned to include a provision on the protection of technological measures which are used by broadcasting organisations in order to protect own neighbouring rights in a transmission. The last meeting of the Committee was held in December 1999. During the preparatory works for the initiative, several Member States and organisations submitted proposals for a possible instrument, including proposals for a WIPO treaty on the protection of the rights of broadcasting organisations. At present, the new instrument is expected to be adopted in the period 2000-2001.

5.1.4. European Union

At the level of the EU, presently only one regulation (apart from the CAD) deals with the legal protection of technological protection devices, i.e. Article 7c Council Directive 91/250/EEC on the legal protection of computer programs (Software Directive).[67]

The scope of Article 7c, however, is rather limited: it deals exclusively with a situation in which technological measures are applied to protect computer programs. This can be, for example, a so-called dongle (software designed to prevent the unauthorised copying of a program). The Directive addresses expressively neither CA devices (although such CA devices as encryption techniques probably may be one means of protection) nor devices used for purposes other than protecting a computer program. Protection is granted, however, irrespective of whether or not remuneration interests are at stake.

Presently, the Draft Proposal for a Copyright Directive is pending.[68] Article 6 would oblige Member States to provide adequate legal protection against the act of circumvention of any effective technological measures.[69] In Section 2, the Draft declares, additionally, unlawful a catalogue of preparatory activities. This catalogue resembles that of the CAD. In this context, the term 'technological measures' means any technology that is designed to prevent or inhibit the infringement of any copyright or any rights related to copyright (Article 6 Section 3 Draft Proposal). Similar to the WCT, WPPT and the Software Directive, protection of a

[67] Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC), OJE No. L 122, 17 May 1991, p. 42; see Annex I section 1.2.1.

[68] Amended proposal for a Directive of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society 10.12.1997, COM (97) 628 final, not yet adopted; see Annex I section 1.2.4.

[69] When banning activities to *circumvent* technological measures, the proposed Article 6 of the Copyright Directive goes further than the CAD, which is focusing on preparatory activities.

technological device is linked to a particular non-remuneration reason the technology serves, i.e. the protection of copyrights or neighbouring rights.

Unlike the CAD and similar to the WCT and WPPT, the Draft Proposal does not address service providers which use a technological device, but rightholders. However, unlike the WCT and WPPT, Article 6 of the Draft Proposal could be of interest to broadcasters and providers of IS services, since it offers protection not only to rightholders and phonogram producers, but also to broadcasters and database producers (see below), in as far as they can claim own intellectual property rights.

This is certainly the case for broadcasters. Neighbouring rights for broadcasters are granted in Council Directive 92/100/EC (Rental and Lending Rights Directive),[70] which recognises certain neighbouring rights of broadcasting organisations in the transmission of a broadcast (irrespective of whether or not the content of the broadcast is subject to own intellectual property protection). In addition, Council Directive 93/83/EC (Satellite Directive)[71] states that neighbouring rights are granted to broadcasters also with respect to satellite broadcasts and encrypted broadcasts. However, the Draft Proposal itself also includes certain neighbouring rights of broadcasters.[72]

Thus, once the Draft Directive has been adopted, providers of broadcasting services may be in a position to claim that devices they have implemented are also intended to protect own intellectual property rights. As a consequence, providers of broadcasting services—irrespective of whether or not their services are provided against payment—may fall under Article 6 of the Draft Proposal, and thus claim protection against acts of unauthorised circumvention of their technological devices *and* against certain preparatory activities. Furthermore, holders of rights in contents transmitted and protected by CA, could claim that activities facilitating an unauthorised circumvention of CA devices implemented violates their rights as granted under the draft Directive (i.e. once the Directive will have been adopted and implemented into national laws). When so doing, service providers probably would enjoy a comparable level of level of protection as enjoy, for example, pay-TV providers under the CAD.[73]

Providers of IS services have not yet been granted specific own rights. In this context, however, the provisions of Directive 96/9/EEC (Database Directive)[74] may be relevant. Under certain circumstances, this Directive grants producers of databases a sui generis (neighbouring) right or even a copyright in a database. Intellectual property rights granted under this Directive also are considered in the framework of Article 6 of the Draft Proposal.

A database in the sense of the Directive can be any collection of information or contents (pictures, sounds, texts, software, information) provided they are arranged in a systematic or methodical way and are individually accessible by electronic or other means. A considerable number of IS services which provide contents seem to operate on the basis of a pre-selected

[70] Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, 19 November 1992, OJE No. L 346, 27.11.1992, p. 61; Annex I section 1.2.2.

[71] Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyrights and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJE No. L 248, 06.10.93, p. 15.

[72] Such as a making-available right and reproduction right.

[73] See Annex I, section 1.2.4.

[74] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, 11 March 1996, OJE No. L 77, 27.03.1996, p. 20; see Annex I section 1.2.3.

and stored collection of contents or information: service providers do not wait for an individual request before acquiring the information, but will already have it stored electronically. This seems to apply to e.g. on-demand services, information services, teletext services, services in the field of e-commerce (e.g. electronic bookshops) and interactive services, such as search engines or online travel agencies.

In addition, at the EC level there are some regulations in the field of broadcasting law which do not address the legal protection of technological measures, but deal with other aspects of access controlled broadcasting services; respectively, standardisation issues (Standards Directive) and the content of such services (Article 3b of the Television Without Frontiers Directive).[75]

5.1.5. Conclusion

As far as there are international regulations on the legal protection of technological devices, they grant protection with view to a particular reason the technology serves. The only exception is Recommendation No. 91(14) of the Council of Europe. This recommendation is, at the same time, the only international initiative which would also address free service providers which use CA devices for non-remuneration reasons. The remaining provisions would protect either remuneration interests (CAD, Conditional Access Convention of the Council of Europe) or subject matters from the field of copyright law.

Most of the other existing regulations can be found in the field of intellectual property law. Regulations in this field do not address primarily the providers of protected services which use a technological device, but a situation in which a device is used to protect a subject matter of copyright law (e.g. a computer program, or works or matters which are subject to neighbouring rights, such as phonograms). Most of these regulations, like the WCT and the WPPT, offer protection only to rightholders, and not to service providers. However, to the extent that service providers are simultaneously the owners of own intellectual property rights either in the content of the service or the service itself, they may possibly benefit from such protection.

This could be the case if the draft Copyright Directive is adopted. Unlike the WCT, WPPT and the Computer Directive, the Draft Copyright Directive principally includes the protection of neighbouring rights in a broadcast and the rights of the database producers; as we have seen, a considerable proportion of providers of IS services may fall under the latter group. Consequently, Article 6 of the Draft Copyright Directive could, once adopted, serve as basis for claims of broadcasters and a number of providers of IS services against acts of circumvention of technological devices, such as the CA techniques they have implemented. This is of particular interest to providers of free CA services, since the draft Copyright Directive does not make protection conditional on the existence of a remuneration criterion.

It should be noted, however, that neither the Draft Proposal nor the other international regulations in the field of copyright address CA devices specifically, but focus in general on "technological measures" (WIPO Treaties), and devices which "may have been applied to protect a computer program" (Software Directive) or are "designed to protect any copyrights

[75] Directive 97/36/EEC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, 30 June 1997, OJE No. L 202 , 30.07.1997, p. 60; see Annex I section 1.2.6.

or any related rights" (Draft Proposal). A precondition for protection is that the devices in question are intended or designed to protect intellectual property rights. In this context, it is worth mentioning that, in principle, access to contents is not an act which is subject to intellectual property rights protection. For this reason, it is still very unclear whether those regulations even address CA devices.[76] On the other hand, the relevant regulations do not explicitly exclude CA devices. Furthermore, the Draft Proposal mentions, inter alia, encryption and scrambling devices, i.e. means of access control. The question whether technological measures in the sense as used in the framework of intellectual property rights also involve CA devices is still subject to heated discussions in Europe, whereas e.g. American and Australian legislators have explicitly included the protection of CA devices in their intellectual property laws.

A related question is whether unauthorised access or activities facilitating unauthorised access would fall under the scope of the Directive. Where a device has been designed for the sole purpose of granting unauthorised access to protected contents or services, this does not necessarily involve a violation of copyrights, since mere access is not subject to copyright law. On the other hand, unauthorised access to a service may coincide in certain cases with the unauthorised use of a work, e.g. downloading the decrypted work (reproduction).

In conclusion, it is unclear to what extent the protection of providers of non-directly remunerated CA services will be completed by international regulations. There is, however, the possibility that particularly Article 6 of the Draft Copyright Directive may offer a comparable degree of protection to broadcasters and a considerable number of IS services which have implemented such devices. However, this will also depend on whether and, if so, how the Directive will be adopted, and how Member States will interpret their provisions and, accordingly, implement them into national laws.

[76] See extensively, Kamiel Koelmann ibid.

Table: Relevant international regulations on the protection of technological devices

Who	Instrument	Field	Subject matter	Free CA services covered	Remarks
Council of Europe	Recomm. 91(14) on encrypted services	Broadcasting law	Protection of CA television services	Yes	Addresses all television CA services, irrespective of whether or not directly remunerated and for which reason CA is used
Council of Europe	Draft Conditional Access Convention	Broadcasting and Information Society law	Protection of directly remunerated CA services (broadcasting and IS services)	No	Not yet adopted Follows pattern of CAD
Council of Europe	Protocol amending the European Convention on Transfrontier Television	Broadcasting law	Free access to contents of major importance for the public	Possibly	CA use in context with protection of minors Does not provide for any protection of CA services
WIPO	WIPO Copyright Treaty	Copyright law	Article 8 protects technological measures used to protect copyrights	No	Addresses only rightholders
WIPO	WIPO Performers and Phonogram Producers Treaty	Copyright law	Article 11 protects technological measures used to protect neighbouring rights	No	Addresses only Performers and phonogram producers
EU	Council Directive 91/250/EEC (Software Directive)	Copyright law	Article 7c protects technological devices used to prevent acts of unauthorised exploitation of computer programs	Possibly	Addresses only situations in which technological devices are used to protect computer programs
EU	Draft Proposal Copyright Directive	Copyright law	Article 6 protects technological devices used to protect works against acts of unauthorised exploitation	Possibly	Addresses also broadcasters as holders of neighbouring rights and producers of databases (important e.g. for providers of IS services)

EU	Directive 95/47 on the use of standards for the transmission of television signals	Technical standards	Access of broadcasters to CA devices on fair, reasonable and non-discriminatory basis	Possibly	No protection of technological devices
EU	Directive 97/36/EC (revised Television Without Frontiers Directive)	Broadcasting law	Article 3b ensures that certain events of importance for the society remain accessible	Possibly	Free access to certain information of public interest Does not provide for any protection of CA services

5.2. Situation in the Member States

5.2.1. Introduction

In the following, specific national legislation on the legal protection of free CA services which use CA devices will be examined and compared. The analysis will be illustrated by a number of tables.

The analysis will include:

- An overview of countries that have adopted specific legislation on the protection of free CA services.
- An examination of the fields of law in which specific laws have been adopted as well as of the subject matter of protection (radio, television broadcasting, IS services).
- The general structure of laws that restrict protection to providers of directly remunerated services or also include non-directly remunerated service providers, on what understanding of the notion of 'remuneration' national regulations are based, and whether national regulations focus on the protection of a particular reasons and whether this is a/these are non-remuneration reason/reasons or not, and if so, what this is/these are. The analysis distinguishes two different questions: 1) Do national laws focus on the protection of directly remunerated CA services, or do they also include free CA services? 2) What reasons to use CA (apart from protection of remuneration interests) do Member States generally consider worthy of protection, i.e. is a distinction made between the *actual* reasons CA may serve? (This against the background that, as the study has shown, even where CA devices are used also for remuneration reasons, this does not exclude that they simultaneously serve additional reasons—provided that the underlying technology is principally neutral).
- An overview of unlawful activities addressed by national laws, as well as the sanctions and remedies provided. This is in order to also examine the question whether Member States distinguish whether the aggrieved party is a provider of directly remunerated or of non-directly remunerated services.
- Whether national regulations have undertaken additional legal initiatives which would take into account the protection of certain third parties' interests possibly affected by the use of CA by service providers.
- A brief overview of to what extent additional legislation is envisaged (particular in the context of the implementation of the CAD) and whether Member States plan to go further than the CAD by including also free CA services.

It should be noted that some countries have adopted specific legislation on the protection of technological measures used to protect copyrightable material. Since these regulations a) do not deal with the protection of services but address a situation in which technological measures are used to protect works in the sense of copyright, and b) it is still under discussion whether such provisions also can be evoked by providers of CA services, such national regulations will be only discussed where this is of particular relevance to the study.

5.2.2. Protection of free conditional access services

Among the Member States that have adopted specific provisions on the legal protection of technical devices, a minority have not made protection conditional on the existence of a remuneration interest—in spite of the fact that a considerable number of these provisions were inspired by Council Recommendation 91(14), which suggests protection for pay as well as free CA services.

Denmark is one of the Member States that grant general protection to free and pay services which use CA devices. The Danish Broadcasting Act protects the contents of encoded radio and TV programmes regardless of the reason a programme is decoded or whether it is provided against remuneration. Denmark is also one of the first Member States where CA devices have already been implemented by providers of free CA services, notably by public broadcasters.[77]

In Finland, specific provisions on the protection of television and radio broadcasting are included in the country's Telecommunications Law. Also here, protection is granted irrespective of whether the service is provided against remuneration.

Belgium is another country where free service providers which use CA devices may also claim protection under specific provisions. However, only non-directly remunerated access controlled cable programmes may benefit from specific protection under the Broadcasting Law. Other broadcasting services (satellite, cable) are only protected if provided against remuneration.

Also, the Irish Broadcasting Act could possibly be interpreted in such a way that it also protects free CA services.

Finally, the current Italian television law protects in general transmissions in encoded form, irrespective of whether or not they are directly remunerated.

A second group of Member States have adopted specific provisions which could be interpreted as covering at least public broadcasting services which use CA devices. In these countries, the notion of remuneration is drafted in a broader way to cover not only the additional fee a pay-TV provider requests in addition to the general broadcasting fee, but the general fee itself (e.g. the Netherlands and the United Kingdom).

France, Sweden and the French-speaking community of Belgium, though providing specific legislation on the legal protection of decoding devices, focus exclusively on the protection of pay-TV providers; in other words, the only beneficiaries of protection are services which are provided against additional remuneration (apart from the general broadcasting fee).

Countries which do not yet have specific provisions on the legal protection of CA devices are Austria, Germany, Greece, Luxembourg, Portugal and Spain. However, these countries may have general legislation which is applicable. By general legislation we mean legislation which is not specifically applicable to services which use CA devices, but nevertheless could be successfully used as a basis for legal proceedings in this field. In most Member States, such a basis probably may be found in civil law, especially in unfair competition law. However, until now, no case law is known where courts had to decide on the applicability of general laws in

[77] See chapter 1.7.

a situation where a free service which uses CA devices was subject to pirate activities. It is therefore difficult to make any observations on applicable general laws in those states.

Of the non-EC Member States examined (i.e. Australia, Canada, Japan and the US), three have specific regulations granting protection to services which use CA devices, irrespective of whether a service is provided against remuneration and the reason the device serves. Here, only Australia restricts the protection of CA devices to a) remuneration interests or b) the protection of intellectual property rights. The Canadian regulation could be interpreted as covering at least public broadcasting services. In addition, the Canadian penal code also protects free CA services in general. Similar to Canada, the US has adopted specific regulations on the protection of CA devices in its Telecommunication Law. Japan's regulation is contained in the country's recently amended Competition Law.

Table 1: Specific protection of free CA services

Country	Specific law	Field of law	Free CA services protected
Austria	/	/	/
Belgium	X	Broadcasting law	(-) (free cable programmes X)
Denmark	X	Broadcasting law	X
Finland	X	Telecommunication law	X
France	X	Broadcasting law (Penal law)	-
Germany	/	/	/
Greece	/	/	/
Ireland	X	Broadcasting law	X
Italy	X	Broadcasting law	X
Luxembourg	/	/	/
Portugal	/	/	/
Spain	/	/	/
Sweden	X	Penal law	-
The Netherlands	X	Penal law	-
United Kingdom	X	Copyright law	-
Australia	X (STILL DRAFT LAW)	Copyright law	-
Canada	X	Telecommunication law, Penal law	- X
Japan	X	Competition law	X
US	X	Telecom. law	X

No specific protection exists
Specific protection: pay-CA services only
Specific protection: free and pay-CA services

" / " = No specific legislation exists; " X" = Yes; " – " = No

5.2.3. Structure of legislation

In the following, it will be examined what general structure specific national laws follow to either focus exclusively on the protection of directly remunerated services or to protect also non-directly remunerated services; in other words, under which conditions providers of CA services are protected.

Where national laws focus on *the protection of providers of directly remunerated services*, three different approaches can be distinguished:

- Some national laws (e.g. those of Australia, Belgium, France and Sweden) protect only services in a situation where they are provided explicitly against remuneration.
- Other laws do not explicitly require that a service is provided against remuneration. Protection is granted, however, only if an unlawful activity has been committed with the intention of not paying a remuneration or fee. This wording indirectly implies that the service is provided against a fee. Such an approach has been taken in the UK and the Netherlands.
- Some laws exclude non-directly remunerated services from the definition of protected services, e.g. the Canadian and the Australian regulation ("encoded broadcasts means a broadcast ... that is made available ... only on payment ... of subscription fees").

The first cluster of laws clearly focus on the protection of a particular kind of service providers, i.e. providers of services which are provided against direct remuneration (as opposed to providers of free CA services). However, in this group national laws do not further distinguish for what additional reasons CA devices are used; in other words, providers of directly remunerated services could also be protected if the device is also used for non-remuneration reasons.

The second cluster of laws protects access controlled services only in a situation where a service is circumvented with the intention of not paying a remuneration. Here, CA devices are seen only in their function of protecting remuneration interests. Where the aggrieved service provider cannot prove such an intention, or a device has been circumvented for another reason (e.g. in order not to provide personal information, to access a programme which was intended exclusively for adults, etc.), probably the laws do not apply.

The third approach is characteristic of the idea which appears to still be dominant in a number of Member States, i.e. that access controlled services are automatically directly remunerated services: the use of access controlled devices is linked to remuneration reasons only, not leaving room for the idea of use of access control techniques by free CA services for non-remuneration reasons.

Where national laws protect *free- and pay CA service providers*, the regulations do not include any reference to a payment criterion, but in general protect all services without determining any particular reason and irrespective of whether the service is provided against remuneration or has been circumvented with the intention not to pay. One exception is where national laws protect technical devices used to protect copyrights (see below).

5.2.4. Notion of remuneration

From the laws examined, apparently no law provides a direct definition of the term "remuneration". From wording and context of the regulations, however, it can be concluded that the notion of remuneration is understood differently from state to state. As we already indicated in the introduction to this study this may have an effect on the actual scope of existing regulations, i.e. on those which make protection conditional on the existence of a remuneration interest.[78] The main underlying question in this context is whether remuneration, in the meaning of national laws, also includes indirect forms of payment, such as payment of the general broadcasting fee which is collected in most Member States[79]—with the consequence that possibly also public broadcasters are protected—or a payment which does not constitute a direct financial contribution between the service provider and the recipient of the service (e.g. financing by sponsoring, advertisements, etc.).

Some national laws suggest that remuneration is understood as a fee which is required *in addition* to the general broadcasting fee. Here, payment of an additional fee is the reason and motive a service provider provides a service, as for example in the Flemish-speaking part of Belgium: "televisieprogramma's … die enkel tegen extra betaling *bovenop de prijs van het kabelabonnement en / of het kijk- en luistergeld worden aangeboden aan het publiek*—"television programmes … which are provided to the public exclusively in return for the payment of an extra fee in addition to the price paid for the cable subscription and/or the viewer's and listener's contribution). A direct relation between payment of a fee and reception of a programme also exists in countries such as France ("*programmes télédiffusés, lorsque ces programs sont réservésà un public déterminé qui y accède moyennant une rémuneration versére à l'exloitant du service*"—"programmes sent, under the condition that those programs are reserved to a limited part of the public which access the programme by means of a remuneration in return for the provision of the service"), Italy ("*servizi televisi numerici a pagamento*"—"numeric television services against payment") and Sweden ("*kodad sänding soms erbjuds mot betalning*"—"encoded transmission where payment is required").

Other wordings leave room for a broader interpretation of the notion of remuneration. One example is the UK regulation. The UK CDPA (Copyright, Designs and PAtents Act) states that protection is not directly conditional on the payment of a fee, but on the existence of an "intent to avoid payment *of any charge applicable to the reception of the programme*" on the part of the (unauthorised) recipient. A similar approach can be found in the Dutch regulation. The notion 'any charge' is broad enough to cover not only direct subscription fees but also indirect general viewing fees, such as a general license fee. Consequently, also public broadcasting programmes may fall under the scope of such provisions, since the reception of public broadcasting programmes is made conditional on purchase of a broadcasting licence. Also the Dutch regulation *("met het oogmerk daarvoor niet volledig te betalen*"—"with the intention not to fully pay") refers to the payment criterion in a rather broad manner, which principally could be applied also to programmes which are financed on the basis of a general license fee. The same can be said about the Canadian regulation, which focuses on the protection of an encrypted subscription programming signal, whereby subscription programming signal means "on payment of a subscription fee or other charge". Whereas such wording probably would not cover commercial programmes, which do not receive any fees from the receivers of the service but are remunerated by advertisers.

[78] Chapter 1.4.
[79] One exception is the Netherlands; due to an amendment of the Mediawet (Media Law), the license fee was scrapped on 1 January 2000.

In conclusion, even where states have adopted legislation on the protection of directly remunerated services, in some of these countries (e.g. the UK and the Netherlands, but also Canada) the law could be interpreted as also covering public broadcasting.

5.2.5. Non-remuneration reasons protected

This section will examine whether Member States generally distinguish between the different reasons CA may serve (rather than distinguish between the groups of service providers—directly remunerated or free—which implement them), and whether the use of CA devices for particular reasons has led to principally different legal solutions.

The former version of a proposal for the CAD defined CA as "any technical measure and/or arrangement whereby access to the service in an intelligible form is made conditional upon a prior individual authorisation aiming at ensuring the remuneration of that service".[80] This means that the CAD would protect CA devices only if they had been designed to serve a particular reason, in this case a remuneration reason. In the final version of the CAD, however, this approach has changed. The Directive now focuses on a particular group of users of services (i.e. providers of directly remunerated broadcasting and IS services) rather than distinguishing between the different reasons CA devices may also serve, as long as they are used by providers of directly remunerated CA services.

The same can be said of the existing national regulations. Although CA devices can be used for a variety of reasons, the qualification of a device is in most cases reason-neutral, i.e. national regulations generally do not focus on the protection of devices that have been designed specifically to serve one or a number of particular reasons (such as secrecy of the protection of minors, etc.) or refer to particular reasons the technology serves. Even where specific legislation does focus on the protection of pay-TV providers only, protection is granted irrespective of which other reasons the device may serve at the same time, as long as the device is used by a provider of a directly remunerated service. As a result, a provider of a directly remunerated CA service which uses a CA device probably could claim protection against circumvention for all possible uses of a device.

One exemption is regulations on technological measures in the field of copyright law. Here, the device normally has to be "designed to prevent or inhibit the infringement of copyright" (Australia) or be "any technology that is designed to prevent or inhibit the infringement of any copyright or any rights related to copyright" (Draft Proposal Copyright Directive). Copyright law is one field of law where national regulation clearly require that a device is designed to serve a particular reason/non-remuneration reason.

Also where national regulations provide general protection for users of CA devices, including free service providers, they do not refer to a particular reason the technology must serve or distinguish between different reasons, with the effect that this would have led to different legal solutions. This means, on the other hand, that national laws do not exclude any particular reasons from protection.

Depending on the field of law in which a regulation has been inserted, it is obvious that national provisions intend in the first place to protect particular interests; e.g. where specific regulations can be found in the field of telecommunications law, confidentiality of

[80] Proposal for a European Parliament and Council Directive on the legal protection of services based on, or consisting of, conditional access COM(97)356 final COD97/0198 (CAD), OJE C 314, 16.10.1997, p. 54.

communication may be one reason to use a device which is clearly protected; in the field of criminal law, the reasons protected may depend on in which section of the law specific provisions have been inserted (e.g. secrecy of communication, theft, fraud, etc.). Irrespective of in which field of law a regulation has been implemented, this does not, however, exclude that also other reasons to use CA are protected.

5.2.6. Service protected

On the national level, most specific provisions on the legal protection of also free CA services (but also the provisions which focus on directly remunerated services only) protect in the first place broadcasting signals. Some national laws also cover radio signals (e.g. Denmark, Finland, Italy, the Netherlands, Sweden and the UK, but also the US, Japan, Canada and Australia), whereas only a small number of national laws are suitable to also protect IS services. This particularly could apply to the Netherlands, France and the UK; however, these regulations focus on the protection of directly remunerated services.

In conclusion, probably no national legislation within the EU protects free IS services which are based on electronic access control.

Among the international regulations examined, only the US (and eventually Canada) appear to have specific legislation which eventually could also be applied to free CA IS services.

Table 2: Protected services

	Television broadcasting	Radio broadcasting	IS services	Only encrypted services
Austria	/	/	/	/
Belgium	X	?	-	X
Denmark	X	X	-	X
Finland	X	X	-	X
France	X	X	X	X
Germany	/	/	/	/
Greece	/	/	/	/
Ireland	X	X	-	-
Italy	X	-	-	X
Luxemb.	/	/	/	/
Portugal	/	/	/	/
Spain	/	/	/	/
Sweden	X	X	-	X
NL	X	X	X	-
UK	X	X	X	X
Australia	X	X	-	X
Canada	X	X	-	X
Penal C:	X	X	?	-
Japan	-	-	-	X
US	X	X	X	-
DMCA:	-	-	-	-

5.2.7. Unlawful activities

Table 3 – Unlawful activities

	Interc.	Manuf.	Import	Distri.	Sale	Rental	Poss. C	Install.	Maint.	Replace.	Advert.	Others	Only com. activit.
Austria	/	/	/	/	/	/	/	/	/	/	/	/	
Belgium	X	X	X	X	X	X	X	X	-	-	X	X	-
Denmark	-	X	X	-	X	-	X	-	-	-	-	X	X
Finland	X	X	X	X	X	X	X	X	X	X	X	X	-
France	-	X	X	-	X	-	X	X	-	-	-	X	-
Germ.	/	/	/	/	/	/	/	/	/	/	/	/	
Greece	/	/	/	/	/	/	/	/	/	/	/	/	
Ireland	X	X	X	X	-	-	X	X	X	-	-	X	-
Italy	-	X	X	X	X	X	X	-	-	-	-	-	X
Luxemb.	/	/	/	/	/	/	/	/	/	/	/	/	/
Portugal	/	/	/	/	/	/	/	/	/	/	/	/	/
Spain	/	/	/	/	/	/	/	/	/	/	/	/	/
Sweden	-	X	-	-	X	X	-	X	X	-	-	-	X
The NL	-	X	X	X	X	-	X	-	-	-	-	X	-
UK	X	X	X	-	-	X	-	-	-	-	X	X	-
Austral.	-	X	-	X	X	X	-	-	-	-	-	X	-
Canada	-	X	X	X	X	X	X	X	X	-	-	X	-
Penal C:	X	X (NOT FREE BA)	-	-	X (NOT FREE BA)	-	X (NOT FREE BA)	-	-	-	-	X	-
Japan	-	-	X	X	X	X	-	-	-	-	-	-	X
US	X	X	-	X	X	-	-	-	-	-	-	-	-
DMCA:	X	X	X	X	-	-	-	-	-	-	-	-	-

Among those states which also protect free CA services, the catalogues of prohibited activities differ considerably from country to country. However, the set of unlawful activities in the context of *pay-CA* services may soon be harmonised throughout the EU by the CAD.

Most of the laws which also protect free CA services cover preparatory activities related to the unauthorised decoder business (e.g. manufacture, import, distribution, sale, rental and possession for commercial purposes). Which specific activities are prohibited varies from country to country. The maintenance, replacement or advertising and such other activities as making available online, exhibition, retransmission of decoded programmes, etc. are rarely included. The situation as regards unauthorised interception is unharmonised. Unauthorised interception is considered unlawful in Belgium, Ireland and Finland, where unlawful activities are not restricted to activities carried out for commercial purposes.

Generally, however, Member States which protect providers of both free and pay services do not treat free CA services differently from directly remunerated services, i.e. prohibit different activities. The same can be said from the non-European countries examined. The only exception to this may be the Canadian Penal Code, where only the interception of non-directly remunerated services is unlawful, rather than any preparatory activities for such

unauthorised interception (such as manufacture, distribution, sale, import, etc. of illicit devices), as was the case for directly remunerated services.

5.2.8. Sanctions and Remedies

Table 4: Sanctions and remedies

	Sanctions Imprisonment	Fines	Admin. Sanctions	Civil remedies
Austria	/	/	/	/
Belgium	-	BEF 26–10.000 (Euro 0,64 – 248)	Confiscation of decoding equipment, forfeiture of profits	?
Denm.	0.5 - 2 years	Unspecified	Confiscation of decoding equipment, forfeiture of profits	Reference to ordinary liability rules
Finland	Up to 6 months	Unspecified	Conditional monetary fines, discontinuation, seizure of economic profit, forfeiture of devices	General civil liability?
France	Up to 2 years	Up to FRF 200.000 (Euro 30490)	Confiscation of devices and advertising material, forfeiture of economic profit	General civil liability?
Germ.	/	/	/	/
Greece	/	/	/	/
Ireland	Up to 2 years	Up to IEP 20.000 (Euro 25395)	Seizure and forfeiture, discontinuation	Specific remedies
Italy	3 months – 3 years	Up to ITL 6.000.000 (Euro 3099)	-	--
Luxemb	/	/	/	/
Portugal	/	/	/	/
Spain	/	/	/	/
Sweden	Up to 6 months	Unspecified	Seizure of devices, forfeiture of economic profit	?
The NL	Up to 3 years	Up to NLG 100.000 (Euro 45378)	Forfeiture of devices and economic profits	?
UK	Up to 2 years	Up to GBP 5.000	-	Copyright remedies
Austral.	Up to 5 years	Up to 500 penalty units	-	Injunctions, damages, compensation for losses
Canada **Penal C:**	Up to 1 year	Up to CAD 20.000	-	Damages, injunctions, Compensation -
Japan	-	Unspecified	-	Injunctions
US	0.5 - 2 years	Up to USD 2.000	-	Damages, Injunctions

Sanctions

Generally, Member States make no differences regarding the scope of sanctions imposed for the circumvention of CA devices where they are used for directly remunerated or non-directly remunerated services. The only exception may be Australia, which provides no penal sanctions for the circumvention of devices used for copyright reasons; however, this is the case with CA devices used by broadcasters to ensure their remuneration interests.

Generally, there are considerable differences in the severity of the sanctions imposed. This applies to regulations protecting also free CA services and to regulations focused on the protection of CA used for remuneration reasons only.

In Europe, sanctions range from a maximum of 6 months of imprisonment in Denmark, Finland and Sweden, to 3 years of imprisonment in the Netherlands. Prison sentences are not always provided for; sometimes national laws only provide for fines. These fines are often unspecified, but where they are specified, they range from BEF 26 (Euro 0,64) in Belgium to DFL 100.000 (Euro 45378) in the Netherlands.

Generally, the laws of non-European countries (e.g. the US, Canada and Australia) provide for considerably higher possible fines and sentences than those in some European countries.

In most states, proceedings can be initiated only by the public prosecutor. Aggrieved parties are often restricted to lodging a complaint with the police.

Administrative sanctions
The majority of national regulations (including those which protect both free and directly remunerated services) also provide for the possibility for courts to order administrative sanctions, such as the seizure of profits and the forfeiture of decoding devices and other equipment. Exceptions could be e.g. Italy and the US, which probably do not provide for any specific administrative sanctions.

Civil remedies
In those Member States that do have specific legislation on the protection of access controlled services, it is often not clear whether and, if so, under which conditions it is possible to start civil proceedings. This applies to countries which protect free CA services as well as those which do not.

Cases of compensatory claims may sometimes be made by the public prosecutor parallel to a criminal case, or in a separate civil proceeding. Often it is unclear who is entitled to start proceedings; most laws are quite vague about who is aggrieved by an action.

Specific civil liability rules apparently exist in e.g. Ireland, Sweden, Australia, Japan, Canada and the US.

In the US, for example, the relevant sections in the Communications Act contain very detailed civil provisions. It is stated that any person concerned by activities which are prohibited may bring a civil action. This includes any person with proprietary rights in the intercepted communication, including wholesale or retail distributors of satellite cable programming, and any person engaged in the lawful manufacture, distribution or sale of equipment. The court is explicitly authorised to grant temporary and final injunctions on such terms as it may deem reasonable in order to prevent or restrain violations. The court may also award actual damages and profits made as a result of the illicit activity, statutory damages for all violations involved in the action, and the recovery of full costs. Furthermore, there is a reversal in the onus of proof in determining the violator’s profits.

The UK refers to the set of civil remedies, which is also available to rightholders.

Where the specific provision itself does not include any references to civil actions (such as in Italy or the Netherlands), probably ordinary liability rules apply. This is clearly the case in Denmark, whose broadcasting law explicitly refers to general liability rules.

In most cases, civil remedies include a claim for damages. However, few countries explicitly provide for the possibility to seek an injunction. In the field of damages, some national laws only provide for the actual damages to be recovered, whereas others also provide for the possibility to claim compensation for loss of profits. Among those countries which protect also free CA services, e.g. the legislation of the UK (to the extent that it protects possibly public broadcasters) and that of Japan explicitly provide for a claim for injunctions, whereas Irish legislation provides for the discontinuation of an infringing activity to be ordered.

However, providers of free CA services are likely to have particular interest in the claim for injunctions and discontinuation of the offending activity. This the more since, as far as providers of free CA services are concerned, the determination of the amount of damages may be difficult. Unlike providers of pay-services, providers of free CA services generally cannot claim a loss of subscription fees (this can be different in the case of public broadcasters claiming the loss of general license fees). In the majority of cases, damages suffered by free service providers will probably comprise indirect losses (such as the loss of information, which is of only indirect economic value) or the costs of replacing a system, loss of confidence, etc. In such a situation, it is not clear how successful claims for damages may be.

5.2.9. Protection under general laws applicable

No cases have been reported concerning providers of free CA services initiating proceedings against acts of unauthorised circumvention of their encrypted services. Thus it is not clear what general laws may apply in such cases, or whether these would be the same laws which are applied to pay-TV services.

Where specific rules do not exist, national courts generally apply the national rules on unfair competition to activities which enable or prepare for the unauthorised reception of CA services (so far repeatedly decided for the field of pay-TV).

It is notable that unfair competition law applies only to commercial illicit activities, since the existing laws on unfair competition generally require the existence of a competitive commercial situation. Furthermore, the importation or possession of decoding equipment as well as all other activities which do not directly affect competition are not considered unlawful.

Under unfair competition law, service providers may claim damages and costs and seek injunctions. Some national courts have repeatedly decided for pay-TV cases that the manufacture and marketing of decoders or pirate cards with the intention of helping third parties to access services without authorisation, can be considered acts of unfair competitive behaviour. By selling illicit devices, the infringer prevents the service provider from earning a fair return on the offered services and from recovering the costs it has incurred. In case of free CA services, however, it is questionable whether the service provider can claim (and prove) the loss of a fair return. Generally, the mere taking advantage of a competitor’s performance does not in itself constitute an act of unfair competition, unless additional circumstances can be proved. National courts have regarded as circumstances indicating unfair competition (in cases where pay-TV providers were involved) the actual hindrance of a competitor, unfairly

profiting because of the development and manufacturing expenses incurred by service providers, as well as the amount of damages or the factual destruction of a closed pay-subscription system.

It remains to be seen how judges will decide in cases concerning the circumvention of free CA services.

Furthermore, on the basis of unfair competition law, claims for damages or costs are generally granted; less often, injunctions or other preventive measures are granted. As mentioned, providers of free CA services generally will primarily have an interest in stopping the unauthorised activity, since damages or loss of profits often will be difficult to prove.

Other general laws which possibly may serve as basis for claims of free CA providers are, for example, national copyright laws, penal laws, telecommunications laws, data protection laws, etc.

As far as national penal laws are concerned, the general prohibitions in national penal codes generally apply only in particular cases of unauthorised access to CA services, one reason being that penal laws generally protect property, privacy or security interests. But preparatory activities as addressed by the CAD (e.g. manufacture, import, sale or installation of illicit devices) do not automatically violate penal laws, since they do not necessarily jeopardise these interests. Copyright laws principally do not deal with unauthorised access to contents or services, but only address acts of unauthorised exploitation. Thus, unauthorised access to services probably would be not unlawful under national copyright laws.

Finally, particularly where CA devices are used by free service providers, this will often be done in order to protect matters which are already subject to own protection under national laws, such as the security and secrecy of communication, data protection, protection of minors, intellectual property rights or protection of firm-owned software and hardware; some of these laws (e.g. data protection laws or communication laws) even impose obligations on service providers to use CA devices.[81] Accordingly, aggrieved parties perhaps may successfully initiate proceedings against circumvention activities on the basis of these laws. It should be noted, however, that in most cases, protection can be claimed only if the circumventing activity has already taken place, i.e. has violated the protected subject matter. In most cases, general laws will not offer any protection against preparatory activities.

But again, one must wait to see how national courts will decide on the applicability of those rules on free CA services.

5.2.10. Trans-frontier aspects

Again, it is difficult to make concrete observations since no cases of the piracy of free CA services have so far been reported. It is likely, though, that the situation would not differ considerably from that in the field of e.g. pay-TV services.

The experiences of providers of pay-TV services have shown that cross-border piracy is a serious problem, particularly where national laws are unharmonised and offer different levels and scopes of protection.

[81] Interestingly, even where particular laws require the use of technological devices in order to protect general interests, these laws generally do not protect such devices against unauthorised circumvention.

To name but some aspects:

- The transfer of valid decoding equipment from the legal owner in one country to an unauthorised owner in another
- The manufacture of pirate cards in countries for which a broadcaster has not licensed any transmission rights, particularly where the country offers no protection to foreign programmes (however, US federal legislation covers both interstate and foreign services).
- Manufacture, distribution, sale, etc. of decoding devices in states where no adequate protection exists
- Making available or publishing the necessary information or password, or distributing decoding software, via the Internet
- Flaws in the field of law enforcement between Member States, such as lack of co-operation, lack of knowledge of foreign legislation, etc.

The position of free service providers is even more difficult, since they receive less specific protection, and unauthorised activities against these providers are prohibited only in a few Member States. This applies even more so to providers of free CA information society services. Furthermore, providers of IS services are—as a consequence of their principally ubiquitous character—even more in danger of being pirated from 'safe-harbour' countries.

5.2.11. Third parties' interests

The use of CA devices in a particular situation may be disadvantageous to or disturb the balance between the parties involved, e.g. with a view to consumers or competitors. Concerns of this kind were the reason for the adoption of a number of regulations also on the level of the EU. For example, Article 3b Television Without Frontiers Directive was adopted in order to prevent the encryption of pay-TV programmes leading to the exercise of exclusive programme rights of broadcasters in a way that would exclude broad sections of the public from access to certain events. Whereas Article 4c of the Standards Directive would control individual monopolists by effectively declaring CA systems to be bottleneck facilities. Recommendation 91(14) of the Council of Europe paid attention to the argument that the encryption of television services may have a negative impact on the rights provided for by Article 10 ECHR.

In the following, it will be examined where national legislators saw the need to adopt, in addition to specific legislation on the protection of CA services, further provisions in order to safeguard existing balances or interests concerned. This chapter should also be seen in context with chapter three – possible impacts of CA use on the Internal Market.

The following overview will take into account all specific legislation, irrespective of whether or not it is restricted to the protection of pay services. In both cases, the underlying problems may be similar. In this context, also the relevant provisions of the DMCA will be introduced. It should be noted that as far as the DMCA provides for exceptions from the prohibitions on circumventing CA, this is primarily to safeguard existing copyright limitations rather than to regulate when the use of CA by service providers may conflict with general interests. Some regulations, however, also seem to take into account the impact of the use of CA on general interests, apart from the sector of copyright, and thus may also be of interest to this study.

National security interests
One issue in the discussion on electronic access control to contents and services is national security interests, e.g. access by the state to contents which may violate national laws and threaten national security interests. This discussion was held, for example, in the context of the use of encryption techniques.

In this context, Australian legislation provides for an exception from protection (of devices to protect copyrights as well as devices to protect remuneration interests) where a circumventing activity has been *lawfully* performed for the purpose of *law enforcement.*

A similar approach can be found in the US Telecommunications Act, where circumventing activities are prohibited "unless ... as may otherwise be specifically authorised by law."

However, both provisions make it clear that acts of circumvention need to be expressly justified by law in order to be lawful.

Free access to certain contents of particular interest for the public
Free access to contents of particular interest for the public is regarded by a number of states as a possible problem when dealing with CA (see also Article 3b Television Without Frontiers Directive).[82]

For example, in this respect Canada felt the need to adopt additional provisions in order to safeguard the accessibility of certain broadcast programmes. Under Canadian law, acts of circumvention are not regarded as unlawful if a) the lawful distributor had the lawful right to make the signal available in a particular area, on payment of a subscription fee or other charge, but b) did not do so, i.e. it made the signal not readily available with the consequence that persons in this area, though willing to pay the required fee or charge, could not access the service, e.g. because the signal was not decoded or the service provider did not made the appropriate decoding devices available. In such a situation, Canadian law allows the decoding of signals without the authorisation of the service provider. This exception, however, does not apply to such preparatory activities as the manufacture, import, distribution, lease, sale, etc. of decoding devices (which may still constitute an offence and are punishable with a fine of up to C$ 25,000).

The Canadian approach reflects a conflict which occurs also in other countries, e.g. in the US, where national laws provide for situations in which the interests of third parties may justify the circumvention of decoding devices, although there is a fear that such a possibility favours the unauthorised decoder market. The Canadian compromise, however, has the disadvantage that only persons who are able to decode a programme on their own (or to develop the necessary equipment) will, in praxis, benefit from this provision.

US law has implemented a different approach, this time concerning the accessibility of public broadcaster's programmes. Under the US Telecommunications Law, it is prohibited to encrypt National Program Services or public broadcasting services which are intended for public viewing, unless at least one unencrypted satellite transmission of any such programme is provided. Public broadcasting services must, in other words, be also be accessible to the public in unencrypted form before the programme may e.g. be part of a digital programme bouquet.

[82] See chapter 3.4.

The provision recognises the importance of public broadcasts for the provision of a certain amount of information as the basis for the public process of opinion-forming. At the same time, it ensures that there will be a certain number of non-encrypted programmes.

Unlike the Canadian approach, the American solution does not provide a "right to decode", but deals with the situation at a deeper level by imposing certain obligations on service providers and even prohibiting the use of CA devices in certain situations. Similarly, the Irish proposal for a broadcasting law states that certain public broadcasting services must remain free-to-air services.

Finally, Denmark shall be introduced here as an example of a member state which has implemented Article 3b Television Without Frontiers Directive into its national laws. Under Danish broadcasting law, the Minister of Culture is empowered to lay down rules to the effect that TV broadcasters may not exercise any exclusive transmission rights to report on events which are of major importance to society in such a way that a substantial part of the public is deprived of following such events on free TV. This means that where providers of encrypted services hold exclusive rights in the transmission of such events, they may not do so within an encrypted service unless a substantial part of the public has access to the transmission. Unlike probably provided for in the Television Without Frontiers Directive, this obligation also applies to free providers of encrypted broadcasting services, such as the Danish public broadcasters DR 1 and 2. In the case of DR 1 and 2, this could mean that DR would first have to distribute the necessary smart cards to the public before it could exercise any exclusive programme rights.

Similar initiatives exist in other Member States that have implemented the revised Television Without Frontiers Directive.

In addition, Denmark—inspired by the Television Convention of the Council of Europe[83]—has also provided for the possibility to restrict the exercise of exclusive programme rights in important events by obliging broadcasters that hold such rights to allow other television broadcasters to also broadcast short excerpts of the reported events and, doing so, safeguard the public's "right to be kept informed".

General decoder market, science, technological development
As already discussed in chapter three, the prohibition of the manufacture, distribution, sale, etc. of devices to decode encrypted signals may have an adverse effect on the general decoder market, particularly where such devices are not primarily designed to circumvent controlled services but may also serve other functions (e.g. multifunctional devices). A related problem is the possible negative impact on science and technological development of the manufacture etc. of decoding devices is generally prohibited.

This aspect has been taken into consideration by, for example, the Japanese regulation on CA. Under Japanese law, under certain conditions the distribution or sale of decoding devices is lawful provided that said devices are exclusively used for experimental purposes. Furthermore, in order not to hinder technological development, the import, distribution, sale and rental of decoding devices is only prohibited where such devices are exclusively used for the purpose of unauthorised circumvention. If a device has multiple purposes, the making available etc. of such a device is not prohibited.

[83] Council of Europe, Protocol amending the European Convention on Transfrontier Television, Strasbourg, 1 October 1998, ETS No. 171; Article 9, see Annex I section 1.2.6.

Finland has also dealt with the problem of a possible hindrance of technological development and of the general decoder market, but via a different solution. Finish telecommunications law provides the possibility to obtain permission from the Telecommunications Administration Centre (TAC) to use a decoding system which normally could also be used to circumvent the encrypted offers of other service providers. TAC is entitled to react to exceptional situations, for example, where a company buys a decoding system in good faith in circumstances where no illegal activity is planned, but later the system is judged to be unlawfully in the possession of that company. At the applicant's request, TAC may grant permission to use the system for e.g. testing purposes.

Security research
The prohibition of circumventing activities may also have a negative impact on security research. The American DMCA states two adequate exceptions, one of which is known as the "hacker paragraph": in this, the circumvention of CA devices and the development of the necessary technological equipment is probably lawful, where this is done in order to identify flaws and the vulnerability of encryption technologies, or for the purpose (here with the authorisation of the owner or operator) of testing the security of a computer, computer system or computer network.

Fair competition
As already indicated in chapter 3.2, the person who controls either access to contents or services or controls the CA technology itself may be in a position to cause distortions of the market and to exclude other service providers from being accessed by the consumer or certain markets. On the European level, such issues are partly addressed by the Standard Directive.

In the framework of the implementation of the CAD, Italy has recently proposed legislation on the issue of standardisation which clearly exceeds the provisions in the Standard Directive.

According to the new draft, providers of access control who provide digital television programmes on their own must guarantee that it is possible to receive with the same decoder all other broadcasting services which are based on access control and provided by other service providers. The draft is a reaction to today's general market tendency for providers to hold property rights in both the technology *and* the contents. This raises the threat of the creation of content monopolies, achieved by establishing technological fences. A service provider that provides own contents and, in addition, controls the technology and the standards under which access to these contents can be controlled, may be in a position to create a factual monopoly if it can thus prevent other services from reaching the consumer.

This is a potential threat not only to the functioning market but also to the plurality of opinions and offers in the media. Once a consumer has chosen a certain technology, it is possible that he/she will refrain from making or not have the possibility to make additional investments (e.g. purchase further decoders, subscribe to other services, etc.) in order to access also the offers of other service providers which use different decoding technologies.

Similar concerns may have inspired the Italian draft provision concerning EPGs and APIs.

The draft includes specific provisions on EPGs and APIs in order to prevent the creation of monopolies and the abuse of dominant positions. EPGs probably must contain concrete information on all offers (including those from competing content providers) and be open to all operators on fair, reasonable conditions. In addition, operators of CA devices apparently must ensure that the APIs they have implemented are open to all service providers. Moreover,

providers of CA devices could be obliged to assist other service providers with the implementation of a particular API.

The Italian draft is one of the first national draft legislation to deal with the issue of EPGs and APIs. Particularly in a situation where the owner of an EPG or API offers own programming contents, there is a danger that it may abuse the technology in order to influence the choice of consumers and favour its own contents or preferences. It can even prevent the contents of competitors from being offered to the consumer. Even if the operator of an EPG or API does not own any own programme content, it nevertheless may find itself in a position to influence which contents are offered to consumers and which are not. An abuse of EPGs or APIs may have a negative effect on competition as well as on plurality.

The Netherlands is another example for a country that has taken specific initiatives in the field of standardisation and fair competition. The Dutch Telecommunications Law stipulates that those who want to offer a CA device must obtain a registration from the OPTA. OPTA's main task is to supervise the provisions which implement the Standards Directive into Dutch law. The registration gives OPTA the possibility to check whether the offered service complies with existing laws.

Consumer protection
Under Italian draft law, providers of CA devices perhaps will also be obliged to provide consumers with sufficient information concerning which broadcasting services (including those from competing service providers) can and—even more importantly—which cannot be received via a particular device (e.g. a set-top box). In addition, devices must be equipped with a programming help function enabling the user to request information about the distribution of any service and the content of a specific digital programme. Similar provisions probably will be found in the Irish draft Broadcasting Law 1999.

By doing so, the proposed provision will have not only an information but also a warning function. Now that it is expected that the offer of digital channels and services will multiply, the Italian legislator apparently felt the need to give consumers the necessary help to handle an offer which may quickly become very difficult to overview.

Privacy
The US also adopted a provision on the protection of (a particular aspect) of privacy in the context of access control mechanisms. According to the DMCA, probably the circumvention of access control devices could be permitted if the technological measure, or the work it protects, is capable of collecting or disseminating information concerning the identity and online activities of a natural person. This could be understood as a right to "self-defence" where CA devices are used to collect information on online behaviour.

Copyright exemptions
One question currently being discussed is the effect of CA devices and other technological protection devices on copyright exemptions and their realisation. Where rightholders use the technology to control access to and the use of works, they may also prevent those who are allowed to access protected works, on the grounds of copyright exemptions, from doing so. The discussion has only just started, and the complexity of the issue is illustrated by the negotiations around Article 6 of the proposed Copyright Directive. Since issues of technological measures to protect intellectual property rights are not primarily subject to this study, however, we will add only a few remarks as far as national laws have particularly dealt with CA devices (not technological measures in general) and copyright law.

Australia and America have already adopted specific provisions on this issue. In Australia, where access to a work is controlled by means of CA, the manufacture, distribution, etc. of decoding devices is not unlawful under the condition that the person supplying decoding devices has signed a declaration stating that the device or service is to be used only for permitted purposes, and also indicates what this purpose is or whether the construction or import of a circumvention device is performed for only a permitted purpose. In this context, permitted purposes must be understood as purposes which are in accordance with Australian copyright exemptions.

The American DMCA provides for more specific exemptions (apart from those already mentioned), e.g. with regard to non-profit libraries, archives, educational institutions and reverse engineering. The DMCA states that the prohibition on the act of circumventing access control measures is subject to an exception that permits non-profit libraries, archives and educational institutions to circumvent solely for the purpose of making a good-faith determination as to whether they wish to obtain authorised access to a work. This exemption is rather limited. Unlike under the Australian regulation, under certain conditions an individual "access right" can be granted. The Australian solution focuses in the first place on preparatory activities.

In addition, the DMCA establishes an ongoing administrative rule-making procedure to evaluate the impact of the prohibitions against the act of circumventing access control measures.

Conclusions
A considerable number of EU Member States have adopted additional legislation which, apart from protecting CA services, takes into account also third parties' possible interests. Such additional provisions can be found in one form or another in all the non-European countries studied (Australia, Canada, Japan and the US).

Where Member States of the European Union with specific legislation on the legal protection of CA decided to adopt additional legislation concerning third parties' interests, the solutions vary strongly from country to country. Similar is true for non-European countries. Together they provide a colourful and rather unharmonised bouquet of ideas reflecting a variety of aspects that may be relevant when dealing with the issue of electronic access control.

Aspects dealt with range from public interest, technological development and requirements of the market, to vital interests of the consumer, such as consumer protection, privacy, access to information, and plurality. Rarely has one and the same aspect been dealt with by more than one country, apart from access to certain information and the problem of hampering the general decoder market and technological development.

But also the way states approached the task of safeguarding third parties' interests differ from country to country. Some countries (e.g. Finland and the Netherlands) have charged independent institutions with safeguarding the interests of the parties concerned. Some states allow under certain circumstances the production of decoding equipment (Australia and Japan) or grant some form of right to circumvent or access (e.g. the US or Canada). Other states have imposed particular obligations for content providers (i.e. whether and, if so, under what conditions they may use CA devices (Denmark and the US)) or on providers of CA devices (e.g. Italy and the Netherlands). Often references to the compatibility with general

laws can be found (e.g. Australia and the US) and by doing so, states kept a door open for the application and enforcement of general laws.

The DMCA seems to be a national provision which also could be understood to deal extensively with CA devices and the safeguarding of the balance of third parties' interests. As noted, in this context the exceptions stated in the DMCA generally do not apply to services which use CA techniques, but to a situation in which works are protected by the use of such techniques. However, only a minority of the exceptions provided for by the DMCA seem to have been inspired by copyright law. The majority of such exceptions probably realises more general interests which exceed the mere field of copyright law and may be of relevance also where CA techniques are used for other reasons than to protect works, such as the aspects of privacy, encryption research and the protection of minors.

The DMCA is also the only one of few regulations which takes into consideration also aspects of the online sector. All other national regulations focus, when formulating exceptions, exclusively on the broadcasting sector and sometimes (even more narrowly) on TV broadcasting, with the effect that adequate provisions for the information society sector are missing.

Finally, it should be noted, that those countries which limit protection to providers of pay services apparently tackle the issue of the interests of third parties not in a different way than countries which protect providers of pay and providers of free CA services do.

Table 5: Third parties' interests taken into account

	Add. legisl.	**Subject matter of protection**	**Method**
Austria	-		
Belgium	-		
Denmark	X	Free access to contents of major interest for the public	Specific obligations for service providers
Finland	X	General decoder market	Installation of independent authority which may grant permission, under certain conditions
France	-		
Germany	-		
Greece	-		
Ireland	-		
Italy	X (proposed)	Fair competition, plurality, consumer protection	Specific obligations for providers of CA devices, services
Luxembourg	-		
Portugal	-		
Spain	-		
Sweden	-		
The Netherlands	X	Fair competition, standardisation	Registration duty for providers of CA devices, services
United Kingdom	-		
Australia	X	National security, law enforcement, copyright law	Exception from prohibition, reference to general laws
Canada	X	Access to certain contents	Access right (under certain circumstances)
Japan	X	General decoder market, science and techn. development	Exception from prohibition
US	X	Free access to public broadcasting, copyright, law	Reference to general laws, specific obligations for

		enforcement, protection of minors, privacy, science, technological development, security research	broadcasting providers, Individual access right (under certain conditions)

5.2.12. Additional legislation planned

Presently, most of EU Member States are in the process of implementing the CAD into national laws. This includes those Member States where specific provisions on the legal protection of CA already exist. The Netherlands claim that existing protection under national laws is sufficient and, therefore, that currently it is not necessary to adopt additional legislation.

In the context of this study, the question of most concern is whether Member States plan to exceed the scope of the Directive by also including free CA services which use CA devices.

The issue of protection of free CA services which use CA has so far brought about no or only marginal discussion in Member States.

Those Member States that do protect free CA services, or at least public broadcasters, will probably maintain this approach in the future. Exceptions are Italy and Finland. As a consequence of the amendment process to implement the CAD, Italy and Finland plan to abolish the protection of free CA services, but will probably introduce a remuneration requirement. This was explained by the recent version of the CAD, which would also make protection conditional on the existence of a remuneration interest.

The example of e.g. Finland is characteristic of the way Member States implement the CAD. Since the Directive concentrates on the protection of CA devices where they are used to protect the remuneration interests of service providers, most Member States seem to prefer to stick to the actual wording of the Directive. This may also be a reason why a possible extension of the scope of the Directive to cover free CA services was not subject to discussion. Accordingly, almost all the Member States that so far do not have specific provisions on the legal protection of CA services will focus, when implementing the Directive, on the legal protection of pay services. One exception could be Austria, which will possibly chose a broader understanding of the notion “remuneration” and, by doing so, implement the Directive in a way that allows also its public broadcasters, which is planning to use CA devices, to be covered.

In the context of access control, only a few countries are using the occasion to regulate additional questions which go beyond the provisions of the CAD and aim at creating an appropriate environment for the fair and balanced use and proliferation of CA. Here, particularly Italy and Ireland are undertaking further reaching initiatives.

Table 6: Future legislation

	Specific protection exists	Future legislation envisaged	Free CA services included
Austria	-	X	?
Belgium	X	?	?
Denmark	X	X	X
Finland	X	X	-
France	X	X	-
Germany	-	X	-
Greece	-	X	-
Ireland	X	X	?
Italy	X	X	-
Luxemb.	-	X	-
Portugal	-	?	?
Spain	-	X	-
Sweden	X	X	-
The NL	X	-	/
UK	X	X	-
Australia	-	X	-
Canada	X	-	/
Penal C:	X	-	/
Japan	-	-	/
US	X	-	/

5.2.13. Conclusions

The legal protection of non-directly remunerated CA services in Europe is still unharmonised. A number of Member States cover free CA services, some laws could be interpreted as covering at least public broadcast services, and others clearly focus on the protection of pay CA services. The exact scope of protection offered depends not least on the how Member States interpret the notion of 'remuneration'. Interestingly, Member States, apart from distinguishing the use of CA devices for remuneration reasons, do not further distinguish what non-remuneration reasons devices are used for in a concrete situation; protection is granted in so far that it is 'reason-neutral' to all *protected* parties, with the effect that no different legal solutions have been adopted as regards the different *non-remuneration* reasons CA may serve. The only exception known are regulations in the field of copyright law, where national laws generally require that a device is specifically designed to protect intellectual property rights.

Whereas the remuneration criterion generally is used to distinguish a particular kind of services rather than a particular reason a CA device must be designed for in order to be protection worthy (i.e. services which are provided against payment of an additional fee).

The situation in non-European countries is not too different. The scope of protection for CA services as granted in Australia, Canada, Japan and America differs considerably from country to country. The US is the only country which apparently protects also non-directly remunerated CA information society services.

As far as the national catalogues of unlawful sanctions are concerned, again the picture is non-uniform, and prohibited activities vary from country to country, including those countries which also protect free CA services. The same applies to the remedies and sanctions offered. In addition, sanctions and remedies are often drafted with view to pay-TV services, and thus do not always fully meet the needs of free CA service providers, even in those countries where they do fall under applicable national regulations.

On the other hand, it cannot be said that Member States which protect both free and directly remunerated services treat these differently as far as the scope of protection and sanctions and remedies granted is concerned. One conclusion could be that the way a service is financed (directly or not directly remunerated) apparently does not principally justify a different legal treatment.

Interestingly, a number of Member States felt the need to adopt, in addition to specific legislation on the protection of CA services, provisions which would take into account certain third parties' interests. As varied and unharmonised as the picture may be, at the national level, specific regulations suggest a variety of other protection-worthy interests (e.g. public interests, or the interests of competitors, the market, science or the consumer/individual), which may raise the need for additional initiatives when dealing with the legal protection of CA.

It is evident that national regulations are, with a few exceptions, still clearly designed with traditional broadcasting services in mind; only a few laws also deal with IS services.

Finally, no cases of the piracy of free CA services have been reported. Thus, it is difficult to predict whether the protection of such services may be completed through the application of general laws, such as unfair competition laws, penal laws, copyright laws and laws on data protection and the security of communication. It remains to be seen how national judges will apply such rules to pirate activities against free CA services. The same must be said for the issue of possible cross-border effects and the question whether existing differences in national legislation weaken the position of providers of free CA services as far as their legal protection is concerned.

6. Conclusions and recommendations

6.1. Conclusions

Conditional access devices can be – and already are – far more than mere payment systems. Basically based on software devices, they are characterised by their multifunctionality and variability, which is also why service providers find it useful to implement them for a variety of non-remuneration reasons.

Among the most important of such reasons are compliance with contractual and statutory obligations, focusing and marketing strategies, user identification, security reasons as well as indirect remuneration reasons.

Some of these economic factors are more often to be found with broadcasters, others are more often to be found with information society services.

In the broadcasting sector, particularly satellite broadcasters but also all forms of digital broadcasters (terrestrial, cable, satellite) have implemented CA for non-remuneration reasons or are planning to do so in the near future. Presently, particularly public broadcasters as free-of-charge service providers are engaged in the implementation of conditional access devices.

Apparently, the most important reason for broadcasters to implement CA devices for non-remuneration reasons are legal obligations, either of contractual or statutory nature. Here, particularly the requirements of the content industry and the use of wide-area transmission techniques raise the need for broadcasters to restrict transmissions to pre-defined territories.

Whereas in the field of information society services, contractual and legal obligations play a smaller role. The field of information society services is less regulated yet. Furthermore, territorial restrictions do not sit well with the principally borderless environment of the Internet, the most important market platform for information society services. In this sector, the identification and security function of CA plays a leading role for a variety of legal and economic reasons.

With both, broadcasting and information society services, CA devices often serve more than one reason at the same time. Accordingly, also providers of pay-TV services have implemented CA devices to serve, apart from remuneration interests, at the same time non-remuneration reasons.

As the analysis of reasons has shown, CA devices, even when implemented for non-remuneration reasons, have an appreciable own economic value for service providers. The economic value of CA is determined by the economic profitability of CA devices as solution for legal or market requirements, in some cases even by the existence of the service itself. Furthermore, CA devices can be also means of developing alternative financing models of services, for example where used for targeted advertising or to ensure indirect remuneration interests which are probably not covered by the CAD.

This latter aspects also indicate that the distinction between remuneration and non-remuneration reasons under the CAD is not always easy to maintain – the lack of a clear definition of the notion of "remuneration" in the CAD adds to the uncertainty. Whereas this study is based upon a narrow definition of remuneration, different interpretations are possible – as a comparison of existing specific national legislation has shown.

Although presently only few data on the use of CA for non-remuneration reasons exist, the economic value of CA together with a number of technical and economic trends and factors indicates an increasing use of CA devices for non-remuneration reasons by providers of broadcasting and information society services. Particularly the increased use of wide-area transmission techniques, the improvement of CA devices, on-going standardisation (particularly in the online-sector) and the convergence of transmission means are incentives for the use of CA for non-remuneration reasons. Whereas the most important economic factors identified are the increasing copyright awareness and exploitation and the trend to narrow-casting instead of broadcasting.

The development, however, could be hampered by piracy of CA systems used for non-remuneration reasons. Although no present danger of piracy of CA devices for non-remuneration devices has been documented yet, there is little reason to believe that free CA services will be considerably less exposed to piracy activities than pay services are. On the other hand, it is not clear yet what influence the general improvement of CA devices will have on the activities of pirates. However, a market for devices which are used for unauthorised access to CA devices for non-remuneration reasons can already be observed to develop.

However, the CAD in its present form focuses exclusively on the protection of CA where it is used to protect remuneration reasons. In other words, only providers of directly remunerated services are provided with protection against piracy activities; providers of free-of-charge services which use the same device for non-remuneration reasons are excluded from protection.

The principal reasons for such unequal treatment are not obvious, particularly where the application of CA devices for non-remuneration reasons is done to realise and protect the economic value of a service.

The unequal treatment under the Directive could put providers of free CA services at a competitive disadvantage, not only because they are excluded from protection, but also regarding the market's confidence in the security of their services. One important aspect in this context affects their negotiating position as regards the content industry: rightholders may well prefer to sell to those who offer the double protection offered by anti-piracy measures applied to directly remunerated CA services. In addition, the lack of protection may increase the costs of unprotected, free CA service providers incur in protecting their services and in seeking remedies from those who pirate their output. Also the development of new free CA services could possibly be hampered if adequate legal protection against pirate activities is denied. Permanent competition with the enhanced and increasingly attractive offers of pay CA providers may, however, require free service providers to develop and improve their offers in order to remain attractive to consumers.

It was also argued that the distinction between remuneration and other reasons may cause legal uncertainty, as the distinction not only makes it difficult to determine what services fall under the CAD but also since it could hamper the efficiency of the CAD concerning the

protection of pay service providers, since it may provoke attempts to circumvent its provisions.

The review of national legislation showed that the protection offered to free service providers in Europe is rather incoherent and incomplete. A number of Member States have adopted legislation extending protection to service providers which use CA for non-remuneration reasons; this was probably a reaction to the Council of Europe Recommendation 91(14). Among these states are Denmark, Belgium (as regards encrypted cable programmes), Finland and Italy. But also major non-EU Countries (such as the US, Japan and Canada) decided not to make a distinction. In other countries, the applicable provisions could be interpreted in such a way that they also cover CA services which are financed indirectly e.g. by public broadcasting fees (e.g. in the UK and the Netherlands).

Member States, apart from the use of CA devices for remuneration reasons, do not further distinguish for what non-remuneration reasons devices are used in a concrete situation – protection is granted insofar " reason-neutral" to all *protected* parties with the effect that no different legal solution have been adopted as regards different *non-remuneration* reasons CA may serve. When implementing the CAD, the majority of Member States will keep to its provisions, i.e. restrict protection to pay services. On the other hand, it should be noted that some states decided, as a consequence of the CAD, to even narrow the scope of existing protection of pay CA services.

The conditions for protection granted for non-remuneration reasons to use CA—particularly the catalogues of unlawful activities, and the sanctions and remedies—differ considerably from one state to the other. Where states decided not to distinguish between free and pay-TV providers which use CA and between the different reasons to use such devices, this did not lead to appreciably different legal solutions than where states concentrated on the protection of the use for remuneration interests; which may also suggest that there is no principal reason to distinguish in protection according to the way a service is financed (as this is presently done e.g. under the CAD).

Due to a lack of case law, it is not yet clear whether national general laws will complete the protection of free CA service providers. Experiences in the field of pay-TV, however, have shown that protection provided under general laws is rather incomplete. In the field of international regulations, particular Article 6 of the Draft Copyright Directive may offer comparable protection to broadcasters and a considerable proportion of providers of IS services. However, the Directive has not yet been adopted and it remains to be seen what effect it will have after it has been adopted and implemented into national laws.

For the same reason, it is still not clear to what extent a lack of harmonised legislation will hamper the development of the Internal Market for such services and the free movement of services. However, from the experiences in the pay-TV sector, one may assume that the lack of sufficient protection and the disparity between national legislation is certainly liable to create obstacles to the development of free CA services similar to those which obstructed providers of pay-TV services—particularly if it turns out that providers of free CA services are threatened to the same or a similar extent by pirate activities.

Most of the Member States with specific legislation on CA services saw already the need to also include in one form or another additional provisions which take into account third parties' interests, such as public interests, access to contents, consumer interests, interests of the market for CA services as well as the general decoder market, security research etc. The

majority of these provisions are modelled on the basis of pay-TV services, and thus do not specifically take into account either free CA services or IS services based on CA. The initiatives of Member States in this field, however, may be a further indicator, that the legal protection of CA services is part of a larger, more complex problem with a variety of possible legal, economic, cultural and technological implications.

The experiences with the effect of increased use of CA on third parties' interests (particular consumers but also the market and its players) are still very limited. Some possible areas of conflict are known from the field of pay-TV, particularly problems in the context of standardisation and the compatibility of CA devices (including EPGs and APIs), fair competition (also between providers of free and pay services), the plurality of choice and access to services. Here, the arrival of a number of new services which use CA devices for non-remuneration reasons may intensify existing problems. Other conflicts may be rather significant for the use of CA devices for non-remuneration reasons, such as matters of consumers' privacy and of data protection, possible influence on consumer's choice and behaviour but also such issues as the availability of accessible contents in the media. Another possible consequence of the use of CA devices for non-remuneration reasons in the broadcasting sector possibly could lead to fragmentation into territorial or language zones. The latter example, however, shows, that the final effects of possible influences are far from being predictable yet. For example, territorial restrictions by means of CA are probably a result of legal obligations and economic considerations such as profit maximisation, which again could have a positive impact on the choice and quality of services.

However, if the CAD were to be extended to cover non-remuneration reasons, this apparently would mean a considerable enlargement of the scope of the Directive, which at the same time would probably undergo a change of character: it would no longer protect only pay-TV providers which use CA devices to ensure their financial viability, but rather the use in general of CA technology for whatever reason by service providers—which possibly has the potential to distort existing balances.

6.2. Recommendations

The current distinction of the protection of CA devices under the CAD between remuneration and non-remuneration reasons is difficult to justify and, furthermore, can give reason for several legal uncertainties.

At the moment, no significant data are available on how the market for services which use CA devices for non-remuneration reasons will develop. However, a number of indicators clearly suggest a tendency towards increased use of CA devices for non-remuneration reasons in both the sector of information society and broadcasting services.

Also, it is difficult to assess whether and, if so, to what extent such a development will be hindered by a piracy problem similar to that in the pay-TV sector and how far existing national laws are capable of dealing adequately with such cases. Apparently, there is no immediate piracy problem which would threaten to seriously hamper the development of CA use for non-remuneration reasons. Therefor, there does not seem to be direct need for action. However, clear trends, based on the research and the outcome of the survey seem to suggest that developments will take a similar course as this was the case with pay-TV.

Therefore, the issue of protection of the use of CA for non-remuneration reasons could be treated as part of the general review of the CAD (Article 7 of the CAD). This would allow a coherent and systematic analysis of the need for further Community action, bearing in mind the economic value of CA devices where used for non-remuneration reasons and also taking into account possible side-effects of an extension on the Internal Market.

As the study has revealed, the use and protection of CA for non-remuneration reasons is part of a far broader context of interests involved with various different implications for the Internal Market and the interests of third parties concerned. Presently, it is still too early to assess the possible impact of CA use on the Internal Market. A serious estimation, furthermore, would require an extensive research which goes far beyond the scope of this study. A general review of the CAD should take into account the complexity of the issue and take the opportunity for further, more extensive research in order to assess the impact of CA use on the general market structures, competition and the interests of the market players, particularly consumer interests.

Probably only some of such aspects would fall directly into scope of aspects which are treated by the CAD. Whereas further aspects may fall in the scope of other, already existing EC initiatives, e.g. in the framework of the Standards Directive and the Television Without Frontiers Directive. Part of an general review of the existing legal framework for CA devices could be whether the existing regulations are still adequate or if further initiatives may be needed.

Research should also pay attention to possible direct and indirect effects of an extension itself on the market, for example on the general decoder market. Initiatives should not lead to a hindrance of either the general decoder market or technical development and encryption research. When envisaging an extension, attention should be paid to this point and also to the definition of “illicit devices” under the CAD.

Furthermore, the opportunity should be taken to examine how to encourage innovation and further standardisation of CA devices which would enhance the general security of the use of such devices.

An extensive review would allow to observe development of piracy in this sector and to assess how national judges will deal with future cases concerning the circumvention of CA devices which are used for non-remuneration reasons, and whether the protection under existing national specific and general laws is sufficient. By then, probably the draft Copyright Directive will have been adopted which would allow to also examine to what extent the provisions of Article 6 of the draft Copyright Directive could complete the protection of the use of CA for non-remuneration reasons.

If the result of such an observation reveals that the use of CA devices for non-remuneration reasons will increase as expected and that the sector will experience considerable problems with piracy, an extension of the Directive could be an appropriate solution to improve the legal situation of free CA services, but also to enhance the general efficiency and practicability of the Directive.

In case, the European Commission decides against an extension, however, a precise definition of the term of “remuneration” would enhance legal certainty and facilitate the application of the Conditional Access Directive.

Annex I

Reports on international regulations and country reports

Index

Introduction 97

1. International regulations 99

1.1 Council of Europe 99

1.1.1. Recommendation 91(14) on the legal protection of encrypted television services

1.1.2. Draft Convention on the legal protection of services based on or consisting of conditional access 102

1.1.3. Protocol amending the European Convention on Transfrontier Television 104

1.2 European Union 105

1.2.1. Council Directive 91/250/EEC on the legal protection of computer programs 106

1.2.2. Council Directive 92/100/EEC on rental and lending rights and on certain rights related to copyright in the field of intellectual property 108

1.2.3. Directive 96/9/EEC on the legal protection of databases 110

1.2.4. Amended proposal for a Directive on the harmonisation of certain aspects of copyright and related rights in the information society 112

1.2.5. Directive 95/47/EEC on the use of standards for the transmission of television signals 114

1.2.6. Directive 97/36/EEC on the co-ordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activity 115

1.3 WIPO 116

1.3.1. WIPO Copyright Treaty 117

1.3.2. WIPO Performers and Phonogram Producers Treaty 118

1.3.3. Further initiatives envisaged 119

2. National regulations 120

2.1 Member States of the European Union 121

2.1.1. Austria 122
2.1.2. Belgium 124
2.1.3. Denmark 128
2.1.4. Finland 131
2.1.5. France 134
2.1.6. Germany 136
2.1.7. Greece 137
2.1.8. Ireland 138
2.1.9. Italy 141
2.1.10. Luxembourg 143
2.1.11. Portugal 144
2.1.12. Spain 145
2.1.13. Sweden 146
2.1.14. The Netherlands 148
2.1.15. United Kingdom 151

2.2. Non-European Countries 154

2.2.1. Australia 155
2.2.2. Canada 159
2.2.3. Japan 164
2.2.4. United States of America 166

Introduction

In the following, an overview is given of the existing national and international regulations which may be relevant in the context of conditional access (CA) services and their protection, particularly where those services use CA devices for non-remuneration reasons.

The following chapter is divided into two subsections. The first reports on relevant international legislation, including the relevant initiatives at the level of the Council of Europe, WIPO and the Council of Europe. Furthermore, where possibly relevant new legislation is pending, the drafts are briefly described.

The second subsection presents in alphabetical order the situation in the Member States of the European Union, as well as reports on Australia, Canada, Japan and the US. The country reports give a systematic overview of the legislation in those states. Within the framework of the reports, we also mention whether additional legislation on the legal protection of CA devices is envisaged (where such plans exist and to the extent that information is available), and if so, whether free CA services will also be covered.

The reports have a common structure, i.e.:

- Introduction
- Details: general information on title, source, date, classification and (where relevant) remarks
- Scope of protection
    - Services protected: the extent to which radio, television broadcasting and IS services are protected
    - Protection of free CA services: the extent to which protection is conditional on the existence of a remuneration interest
    - Reasons protected: specific reasons focussed (or not focussed) on by existing legislation
    - Definitions: relevant definitions as far as such are provided by law
    - Unlawful activities: activities prohibited under national laws
    - CA services and the interests of third parties: additional legislation providing for specific provisions/obligations with a view to the balance between interests concerned
    - Sanctions/Remedies: penal, administrative and civil remedies, and planned sanctions
    - General legislation: applicable general legislation respectively where no specific legislation exists
    - Case law: specific case law dealing with the circumvention of CA devices when used for non-remuneration reasons/initialised by providers of free CA services
- Additional legislation envisaged: further initiatives envisaged, particularly in the course of the implementation of the Conditional Access Directive (CAD) into national laws, with special emphasis on the question whether such initiatives also include free CA services which use CA devices.

Generally, all points will be addressed. Where certain points are not relevant or not addressed in a country, however, they will not be mentioned.

In the context of this study, the overview focuses primarily on legislation on the legal protection of technological access control techniques. Nevertheless, we complete the overview by briefly discussing other initiatives which are of relevance when dealing with the issue of CA, such as the Standards Directive and Article 3b of the Television Without Frontiers Directive.

As far as Member States have adopted specific legislation on the protection of technological measures in the field of copyright law, those provisions will be reported only where this is of particular interest for this study. This is because provisions on the protection of technological measures in the field of copyright law, unlike the CAD, do not address services using CA but a situation in which technological measures (not necessarily CA devices) are used to protect a work in the sense of copyright (see also “European Union”).

It should be noted, however, that existing legislation can be hard to find, because the subject is classified under very different legal headings, e.g. telecommunications, copyright, anti-piracy problems, counterfeiting, computer criminality, specific legislation, or plain penal or civil law. The same applies to initiatives: the subject is not always dealt with by the same ministry.

1. International regulations

1.1. Council of Europe

1.1.1. Recommendation No. R(91)14 adopted by the Committee of Ministers of the Council of Europe on 27 September 1991 on the legal protection of encrypted television services

Introduction

In September 1991, the Council of Europe adopted Recommendation No. R (91)14 on the legal protection of encrypted television services. This recommendation is the only known international regulation on the legal protection of access controlled services that does not distinguish between encryption used for remuneration and that used for other reasons. It thus protects both pay and free CA broadcasting services to the same extent.

On the basis of the Recommendation, specific legislation on the legal protection of encrypted television services has been implemented by a number of Member States of the Council of Europe, e.g. Denmark, Finland, France, Ireland, Switzerland and the UK.

Details

Title: Recommendation No. R(91)14 adopted by the Committee of Ministers of the Council of Europe on 27 September 1991 on the legal protection of encrypted television services
Date: 27 September 1991
Source: http://www.coe.fr/cm/ta/rec/1991/91r14.htm

Scope

Services protected
The Recommendation deals exclusively with encrypted television services. It does not deal with either radio broadcasting or IS services.

In this context, 'encryption' is understood in a broad sense to cover a variety of techniques, including coding and scrambling. Whether it is questionable if the recommendation also covers other means of access control such as password systems.

Interestingly, the Recommendation states that organisations providing encrypted television services have the responsibility to use the best available encryption techniques.

Free CA services protected
Although the Recommendation mentions that especially pay-TV services use encryption techniques, it addresses all television services which use encryption techniques, including free-of-charge television broadcasting services.

Reasons protected
The Recommendation does not distinguish between the reasons for which encryption techniques may be used. In the Explanatory Memorandum to the Recommendation, the Council of Europe explicitly states that broadcasters may wish to restrict the audience of its programmes for such reasons as those of copyright and neighbouring right. Furthermore, particularly in the case of services for a professional vocation, broadcasters may wish to restrict access to programmes to a closed user group which has particular interest in the broadcasts (e.g. in the case of medical programmes). The Explanatory Memorandum states that even in cases where a programme service is not encrypted for direct financial reasons but with view to restricting its reception area to a given territory or audience, illicit access to that service entails legal uncertainty for the broadcaster concerned, even though such access may not cause it a direct financial prejudice. In addition, the broadcaster may expose itself to legal action from rightsholders in the works and other contributions incorporated in these programmes, on the grounds that the actual transmission area exceeds that foreseen in the contracts negotiated with the rightsholders (Explanatory Memorandum, No. 6).

Definitions
'Encrypted services' are "all television services transmitted or retransmitted by any technical means, the characteristics of which are modified or altered in order to restrict access to a specific audience".

'Decoding equipment' is "any device, apparatus or mechanism designed or specifically adapted, totally or partially, to enable access 'in clear' to an encrypted service", that is to say, without the need to modify or alter its characteristics. The definition also refers to cases where access is only possible if the decoder is coupled to other pieces of equipment or devices. The definition also applies where a single piece of equipment provides various functions, one of them being to provide access to an encrypted service (Explanatory Memorandum, No. 15).

Unlawful activities
Under the Recommendation, the following activities are considered unlawful:
- manufacture
- importation
- distribution
- commercial promotion and advertising or manufacture, importation or distribution
- possession for commercial purposes of decoding equipment.

However, it is left up to Member States to determine whether private possession is an unlawful activity.

CA services and the interests of third parties
In the Explanatory Memorandum, it was indicated that there may be some concern as regards the principle of freedom of expression and free access to information. The opinion was expressed, however, that the freedom to receive broadcasts cannot be construed as an entitlement for the public to override the legitimate interests of those with an economic interest in the provision of television services.

Sanctions/ Remedies

Sanctions
Member States of the Council of Europe should make provisions for penal sanctions in case of unlawful activities.

Administrative measures
The same applies to administrative sanctions. Provisions should include the search of premises and the seizure of any material relevant to the investigation, including the decoding equipment and the means used for its manufacture. In addition, destruction or forfeiture of decoding equipment should be provided for, as should the forfeiture of any financial gain.

Civil remedies
Member States should also provide provisions allowing the injured encryption organisation to institute civil proceedings, notably to obtain injunctions or damages, claim profits as well as the seizure, destruction or delivery of decoding equipment, in as far as domestic law permits this.

1.1.2. Draft Convention on the legal protection of services based on or consisting of conditional access

Introduction

The Council of Europe is currently finalising and preparing for adaptation the Draft Convention on the legal protection of services based on or consisting of conditional access.

Details

Title: Draft Convention on the legal protection of services based on or consisting of conditional access
Date: Not yet adopted
Source: -

Scope of protection

Services protected
Similarly to the EC Conditional Access Directive (CAD), the Convention deals with broadcasting and IS services which are offered against payment and on the basis of CA, as well as CA services on their own.

Free CA services protected
The Convention, again similar to the CAD, does not address free CA services.

Reasons protected
In the Explanatory Report to the Draft Convention, the Council makes clear that other reasons than to ensure remuneration interests for encrypting services and controlling access (such as security, privacy or the protection of rightsholders) do not come within the scope of the Convention. Although it was acknowledged by the authors of the Convention that the encryption of services for the purpose of protecting rightsholders deserved particular attention, it was considered preferable to deal with this question in a separate legal instrument. In this context, it was referred to the 1996 WIPO Treaties (WCT and WPPT Treaties) and the Draft Copyright Directive of the European Community.

Definitions
'Protected service' means any of the following services if they are provided against remuneration and on the basis of CA:
- television programme services, as defined in Article 2 of the amended European Convention on Transfrontier Television
- radio broadcasting services, meaning radio programmes intended for reception by the public, transmitted by wire or over the air, including by satellite
- IS services, understood as those offered by electronic means, at a distance and at the individual request of a recipient of services or
- the provision of CA to the above services considered as a service in its own right.

Unlawful activities

The Convention declares unlawful certain preparatory activities with respect to the commercial illicit decoding business, such as the manufacture, production, importation, distribution, sale or rental, possession (for commercial purposes), installation, maintenance or replacement, as well as the commercial promotion, marketing or advertising of illicit devices. This catalogue of unlawful activities closely resembles that of the activities which are subject to the CAD.

Sanctions/Remedies

Sanctions

Unlike the CAD, this convention requests Member States to adopt criminal or administrative sanctions. Measures shall be effective, dissuasive and proportionate to the potential impact of the unlawful activity.

In addition, Member States shall enable the seizure and confiscation of illicit devices and/or the promotional, marketing or advertising material used in the commission of an offence, as well the forfeiture of any profits or financial gains resulting from the unlawful activity.

Civil Remedies

Member States shall ensure that providers of protected services whose interests are affected by an unlawful activity have access to appropriate remedies, including bringing an action for damages and obtaining an injunction or other preventive measure, and where appropriate, applying for the disposal of illicit devices outside commercial channels.

1.1.3. Protocol amending the European Convention on Transfrontier Television

Details

Title: Protocol amending the European Convention on Transfrontier Television
Date: October 1998
Source: ETS No. 171, also http:// www.coe.fr/eng/legaltxt/171e.htm

Summary

Although the amended European Convention on Transfrontier Television does not deal with the legal protection of CA devices, it states certain requirements concerning the content of access-controlled services and is thus worthy of mention in the context of this study.

Article 9 obliges Contracting Parties to examine and, where necessary, take legal measures such as introducing the right to short reporting on events of high interest for the public to avoid the right of the public to information being undermined due to the exercise by a broadcasters within its jurisdiction of exclusive rights for the transmission or retransmission, within the meaning of Article 3, of such events.

Furthermore, a new Article 9*bis* has been introduced which provides, with reference to the Convention for the Protection of Human Rights and Fundamental Freedoms, that Contracting Parties may ensure by appropriate means that a broadcaster within its jurisdiction does not broadcast on an exclusive basis events which are regarded by that Party as being of major importance for society in such a way as to deprive a substantial proportion of the public in that state of the possibility of following such events by live coverage or deferred coverage on free television. The Convention also suggests, similar to the revised Television Without Frontiers Directive,[84] the drafting of lists of national or non-national events which are considered by a Party as being of major importance for society.

[84] See Annex I, Section 1.2.6.

1.2. European Union

1.2.1. Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs

Introduction

Article 7c of Directive 91/250/EEC (Software Directive) addresses technological measures used to protect computer programs. The provision does not necessarily focus on CA techniques, although CA devices (such as encryption techniques) are certainly one means with which to protect computer programs.

Details

Title: Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (91/250/EEC)
Date: 14 May 1991
Source: OJE No. L 122, 17 May 1991, p. 42
Classification: Copyrights and neighbouring rights

Scope of protection

Services protected
Protection granted under the Software Directive does not address services which use technical measures, but the particular situation where technical devices are used to protect a computer program. In doing so, the Directive focuses on a specific function of technical measures, i.e. the protection of computer programs. Technical measures in the sense of the Directive are probably not necessarily CA devices, although these are not explicitly excluded (e.g. encryption techniques). To give an example, a technological measure in the sense of the Directive may be a so-called dongel (software designed to prevent unauthorised copying).

The Directive may be of relevance to particular fields of e-commerce, particularly the increasingly important secure delivery of software via the Internet. However, the Directive does not cover such services resulting from a software-based working process, such as the final process of data or content transmission, the realisation of a text, sound or picture, etc. In other words, it focuses exclusively on the protection of software, not on a result the software realises.

Beneficiaries of protection are all natural or legal persons who are rightsholders in the thus protected computer program.

The Directive probably does not protect CA software itself where a CA technique is used to secure a program. The software which belongs to a CA device realises the technical protection, and thus is not software protected by a technical measure but is the technical measure itself.

Reasons protected
The Directive focuses on the protection of computer programs as subject to copyright law protection.

Unlawful activities
Article 7 (c) Software Directive prohibits any act of putting into circulation, or the possession for commercial purposes of, any means where the sole intended purpose is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

Sanctions/Remedies
The Directive does not suggest any specific sanctions but obliges Member States to provide appropriate remedies.

1.2.2. Council Directive 92/100/EEC of 19 November 1992 on rental right and lending rights and on certain rights related to copyright in the field of intellectual property

Introduction

The Rental and Lending Rights Directive does not address the issue of the protection of CA techniques. The importance of this Directive lies in the fact that it recognises certain exclusive rights of broadcasting organisations (neighbouring rights) in the broadcasting transmission, rather than in the content of the transmission.

Should the proposed Copyright Directive[85] be adopted, neighbouring rights protection of broadcasters could be completed by Article 6 of the Directive, i.e. the protection of technological measures which are used by rightsholders (here, broadcasters) in order to protect their rights. In other words, broadcasting organisations could claim that certain unauthorised activities with regard to technological measures are unlawful under Article 6 of the Draft Directive.

Details

Title: Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (Rental and Lending Rights Directive)
Date: 19 November 1992
Source: OJE No. L 346, 27.11.1992, p. 61
Classification: Copyrights and neighbouring rights
Remarks: Neighbouring rights of broadcasting organisations will probably also be subject to Article 6 of the proposed Copyright Directive (protection of technological measures)

Scope of protection

Services protected
Subject to protection are broadcasting organisations irrespective of whether their broadcasts are transmitted by wire or over the air, including by cable or satellite. Also protected are cable operators who provide own programming.

However, it is not quite clear whether also encrypted broadcasts are included. According to Article 1 Satellite Directive,[86] the Rental and Lending Rights Directive applies at least to programme-carrying satellite signals which are encrypted, provided the means for decrypting the broadcast are provided to the public by the broadcasting organisation or with its consent. It is not clear, however, whether this also applies to encrypted terrestrial and cable broadcasting.

[85] See Annex I, Section 1.2.4.
[86] Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyrights and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJE No. L 248, 06.10.93, p. 15.

The Directive does not cover IS services.

Free CA services protected
The guarantee of exclusive rights is given irrespective of whether or not a broadcasting service is provided against remuneration.

Unlawful activities
The Rental and Lending Rights Directive grants protected broadcasters certain exclusive rights, based on which broadcasters can prevent certain acts of unauthorised exploitation/piracy. These exclusive rights are a fixation right, a reproduction right and a right of communication to the public. However, the Directive does not address the protection of any technological measures.

Exceptions
The rights of broadcasters are subject to such limitations as private use, short excerpts, ephemeral copies and educational or scientific purposes.

Sanctions/Remedies
Sanctions and remedies conform to the provisions of general national copyright laws.

Remarks
Protection may eventually be completed by Article 6 Draft Copyright Directive (protection of technological measures), with the result that technological measures such as CA devices may also be protected (see below, also "Database Directive") when applied by broadcasters in order to protect a broadcasting transmission against pirate activities.[87]

[87] See section 5.1.4.

1.2.3. Directive 96/9/EEC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

Introduction

The provisions of the Database Directive may have particular relevance to the field of IS services, especially with regard to information and on-demand services. This is because a considerable part of IS services[88] could qualify as a database and thus be protected by the Directive.

Details

Title: Directive 96/9/EEC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
Date: 11 March 1996
Source: OJE No. L 77, 27.03.1996, p. 20
Classification: Copyright and neighbouring rights
Remarks: Intellectual property rights in databases are possibly also included in Article 6 of the proposed Copyright Directive (protection of technological measures)[89]

Scope of protection

Services protected
The Database Directive does not address services but databases. According to Article 1 (2) Database Directive, 'database' shall mean a collection of independent works, data or other materials provided they are
- arranged in a systematic or methodical way, and are
- individually accessible by electronic or other means.

A database in the sense of the Directive can thus be any collection of information or contents irrespective of whether these are pictures, sounds, literature, articles, online journals, software tools, computer games, share quotation data, etc.

In this context, it must be noted that certain services (particularly such IS services as on-demand or interactive services) may be provided on the basis of a collection of relevant data and at the individual request by the user, i.e. a database in the sense of the Directive.[90] The crucial feature of e.g. an on-demand service is that the individual user requests a certain content (film, piece of music, game, software, etc.) which he/she previously selected from the offer of the service provider. Generally, a service provider will not wait until content,

[88] Council Directive 83/189/EEC laying down a procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 94/10/EC, OJE No. L 100, 19.04.1994, p. 60, defines IS services as any service provided at a distance, by electronic means and at the individual request of a service receiver.
[89] See Annex I, section 1.2.4.
[90] As opposed to e.g. information provided within the framework of a live service, where on the side of the service provider a natural person is involved and deals directly with the request.

information, etc. is requested by an individual user before offering it, but will already have it secured and stored electronically. In other words, the service is operated on the basis of a collection of such contents. The contents in question are, necessarily, also individually accessible since they can be requested individually. Provided that such a collection of contents is arranged in a certain systematic or methodical way, or at least involves a substantial investment, the service provider may thus be considered a producer of a database in the sense of the Directive, and as such enjoy exclusive rights.

Free CA services protected
The guarantee of exclusive rights is given irrespective of whether or not a database is provided against remuneration.

Unlawful activities
The Database Directive grants producers of databases certain exclusive rights, based on which such producers can prevent certain acts of unauthorised exploitation.

Where a collection qualifies as a database in the sense of the Directive, it may under certain circumstances[91] be protected by copyright. As a result, the author of the database is granted certain exclusive copyrights with respect to the database as a whole.[92] Apart from that, even if a database does not qualify for copyright protection, its maker may be granted the right to prevent extraction and/or reutilization of the whole database or a substantial part of it (*sui generis* right). The *sui generis* right in databases is granted if qualitatively and/or quantitatively a substantial investment was involved in either obtaining, verifying or presenting the contents.[93]

Technical devices and the interests of third parties
The rights of broadcasters are subject to limitations, such as private use, educational or scientific purposes, public security or other exceptions under national law.

Sanctions/Remedies
Sanctions and remedies conform to the provisions of general national copyright laws.

Remarks
Again, protection may eventually be completed by Article 6 Draft Copyright Directive (protection of technological measures), with the result that technological measures which a service provider implement, such as CA devices may also be protected (see below).

However, the provisions of the Database Directive will not apply to IS services which are not based on a pre-prepared database, such as live streaming of web-radio programmes, interactive online games or online orders where the delivery is performed off-line. The Directive probably also does not apply to radio or television broadcasting, even if the transmission is provided on the basis of stored pre-made copies, since the contents of the programme are not individually accessible.

[91] Copyright protection of databases is made conditional on the existence of a certain selection or arrangement of the contents of the database which expresses the author's own intellectual creation (Article 1 (2) Database Directive).
[92] E.g. a reproduction right, translation, adaptation, arrangement, distribution of parts or copies of parts of the database to the public, communication to the public, etc.
[93] Note that the copyright protection of databases does not extend to their contents.

1.2.4. Amended proposal for a Directive of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society

Introduction

Within the framework of the proposal for a copyright Directive, it was proposed to introduce provisions on the legal protection of technical measures intended to protect copyright. The technical copyright protection measures referred to in the Draft Proposal are not necessarily CA techniques; however, certain CA devices such as encryption and scrambling techniques could constitute at least one form of technological measures as addressed by the proposal (apart from other forms of protection devices, such as anti-copying mechanisms, ECMS, etc.).[94]

Details

Title: Amended proposal for a Directive of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society 10.12.1997, COM (97) 628 final
Date: Not yet adopted
Source: -
Classification: Copyright and Neighbouring rights

Scope of protection

Services protected
The Draft Directive does not address certain services which use technological devices, but a situation where technological measures are used by authors or holders of neighbouring rights in order to protect copyrights, neighbouring rights or the *sui generis* right in databases.

The precondition for protection is that the devices in question are *designed to protect intellectual property rights.*

Reasons protected
The Draft Directive protects copyright and neighbouring rights.

Unlawful activities
According to the proposed Directive, protection is granted (unlike under the CAD) not only against commercial preparatory activities but also against the act of circumvention itself. Member States shall "provide adequate legal protection against the circumvention without authority of any effective technological measures designed to protect any copyright or any

[94]See definition technological measures: "Technological measures shall be deemed 'effective' where the access to or use of a protected work or other subject matter is controlled through application of an access code or any other type of protection process which achieves the protection objective in an operational and reliable manner with the authority of the rightholders. Such measures may include decryption, descrambling or other transformation of the work or other subject matter."(Article 6 (2) Amended Proposal).

rights related to copyright." Whereas the proposed catalogue of preparatory commercial activities resembles the CAD and comprises probably the manufacture, import, distribution, sale, rental, possession and advertisement of illicit devices. Their installation, maintenance, replacement is not included.

The notion of "illicit devices" is, in comparison to the CAD, more restrictively defined as "devices, products or components or the provision of services, carried out without authority, which: a) are promoted, advertised or marketed for the purpose of circumvention of, or b) have only a limited commercially significant purpose or use other than to circumvent, or c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures."

Secondly, also the notion of technological measures is, at the first glance, more restrictive than this is the case for CA devices in the sense of the CAD: Under the proposed Copyright Directive, devices must be "effective". It is still unclear, what "effective" in this context means. In the latest official proposal it was suggested to consider "effective" devices "where access to or use of a protected work or other subject matter is controlled through application of an access code or any other type of protection process which achieves the protection objective in an operational and reliable manner with the authority of the rightholders. Such measures may include de-cryption, descrambling or other transformation of the work or other subject." The definition, thus, could be interpreted in a way as to refer to CA devices in general.

Procedural provisions
However, where CA devices are used to protect exclusively the intellectually property rights of a third person, it is questionable whether a mere service provider can claim protection. Generally, intellectual property right entitles only the rightsholder (i.e. not third parties) to certain rights. This poses no problem, at least where service providers such as broadcasters use CA devices in connection with own copyrights or neighbouring rights.

Sanctions/Remedies

Sanctions
Similarly to the CAD, it was proposed to oblige Member States to ensure appropriate sanctions and remedies. The sanctions thus provided for shall be effective, proportionate and dissuasive and acts as a deterrent for further infringement.

Civil remedies
Also the catalogue of remedies proposed resembles the CAD and includes claims for damages and/or injunction as well, where appropriate, seizure of infringing material.

Technical devices and the interests of third parties
It is likely that the application of CA devices in the context of copyrightable material will be subject to certain restrictions as far as this is necessary to warrant the exercise of certain exemptions by users of works or services. In so far, the final version of Article 6 of the proposed Copyright Directive must be awaited.

Remarks
Summarising, the level of proposed protection for users of technological measures could resemble the level of protection CA users enjoy under the CAD – with some differences, e.g. a stricter definition of illicit devices.

1.2.5. Directive 95/47/EEC of the European Parliament and of the Council of 24 October 1995 on the use of standards for the transmission of television signals

Details

Title: Directive 95/47/EEC of the European Parliament and of the Council of 24 October 1995 on the use of standards for the transmission of television signals (Standards Directive)
Date: 24 October 1995
Source: OJE No. L 281, 23.11.1995, p. 51
Classification: Technical standards

Summary

The so-called Standards Directive deals with another aspect of CA, i.e. the standardisation of CA technologies. One aim of the Directive is to ensure a certain degree of compatibility and fair competition between competing systems. Article 4 (c) Standards Directive obliges providers of CA devices for digital television services to offer to all broadcasters, on a fair, reasonable and non-discriminatory basis, technical services which will enable the broadcasters' digitally-transmitted services to be received by viewers authorised by means of decoders administered by the service operators, and to comply with Community competition law, in particular if a dominant position appears. This is in order to ensure fair competition not only between the producers of CA devices but also between CA producers and digital television broadcasters.

Note that the Standards Directive does not apply to CA within the framework of IS services. Furthermore, it is also not clear whether the Directive applies to CA devices which are used for non-remuneration reasons. The recitals to the Directive seem to indicated that is was drafted with pay-TV in mind.

1.2.6. Directive 97/36/EEC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the co-ordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities

Details

Title: Directive 97/36/EEC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the co-ordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (Revised Television Without Frontiers Directive)
Date: 30 June 1997
Source: OJE No. L 202 , 30.07.1997, p. 60
Classification: Broadcasting law

Summary

Although Article 3a of the revised Television without Frontiers Directive does not deal with the legal protection of CA devices, it states certain requirements concerning the content of access-controlled services and is thus worthy of mention in the context of this study.

The provision obliges Member States to ensure that broadcasters do not broadcast on an exclusive basis events which are regarded by that member state as being of major importance to society. Broadcasters may not deprive a substantial proportion of the public in that member state of the possibility to follow such events via live coverage or deferred coverage on free television. The underlying intention is to warrant the conditions for a free flow of information relevant to the process of public opinion-making.

Note that there are no such obligations as regards the transmission of important events within the framework of IS services (e.g. webcasting). Free access to certain online contents is still not subject to either European or national legislation.

'Free television' in the sense of the Directive means "broadcasting on a channel, either public or commercial, of programmes which are accessible to the public without payment in addition to the general broadcasting fee or the basic tier subscription fee to a cable network." However, it is not clear whether services which are encrypted for non-remuneration reasons also fall under the definition of 'free television'.

1.3. World Intellectual Property Organisation (WIPO)

1.3.1. WIPO COPYRIGHT TREATY

Introduction

Article 11 WIPO Copyright Treaty addresses the legal protection of technological measures when used by authors to protect copyrights. The regulation does not necessarily address CA devices. On the other hand, perhaps CA also can be used for reasons of copyright protection.

Details

Title: WIPO Copyright Treaty (WCT)
Date: 20 December 1996
Source: http://www.wipo.org/eng/main.htm

Scope

Services protected
Article 11 WCT deals with technological measures used to protect copyrights. Note that the WCT focuses on authors only and thus does not cover e.g. broadcasters which use CA as means to protect their neighbouring rights in the broadcasting transmission.

Free CA services protected
Where providers of free CA services use technological measures to protect own copyrights in the content of the transmission, they may fall to the same extent under the provisions of Article 11 WCT as providers of pay services which use the technology for the same purpose, irrespective of the existence of any remuneration interests.

Reasons protected
The provision focuses exclusively on the protection of copyrights.

Unlawful activities
Article 11 WCT addresses in more general terms the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights and with restrict acts (in respect of works) not authorised by the authors concerned or permitted by law. The notion ‘permitted by law’ refers primarily to the set of exemptions generally provided by copyright laws.

Sanctions/Remedies
Member States shall provide adequate legal protection and effective legal remedies. The WCT leaves Member States free to decide what remedies are appropriate.

1.3.2. WIPO Performance and Phonograms Treaty

Introduction

Similar to Article 11 WCT, Article 18 WIPO Performance and Phonograms Treaty (WPPT) deals with the legal protection of technological measures used to protect intellectual property rights of performers and phonogram producers.

Details

Title: WIPO Performance and Phonograms Treaty (WPPT)
Date: 20 December 1996
Source: http://www.wipo.org/eng/main.htm

Scope of protection

Services protected
Article 18 WPPT deals with technological measures to protect certain neighbouring rights. Again, the provision does not address particular services which use technological measures than a situation in which devices are used to protect certain neighbouring rights. Note that the WPPT focuses on performers and phonogram producers only, and thus does not cover e.g. broadcasters which use CA as means to protect their neighbouring rights in the broadcasting transmission.

Free CA services protected
Where providers of free CA services use technological measures to protect neighbouring rights in phonograms and performances, they may fall to the same extent under the provisions of Article 18 WPPT as providers of pay services which use the technology for the same purpose, irrespective of the existence of any remuneration interests.

Reasons protected
The provision focuses exclusively on the protection of neighbouring rights in phonograms and performances.

Unlawful activities
Article 18 WPPT addresses in more general terms the circumvention of effective technological measures that are used by performers and phonogram producers in connection with the exercise of their rights and which restrict acts (in respect of works) that are not authorised by the parties protected or permitted by law. The notion ‘permitted by law’ refers primarily to the set of exemptions generally provided by copyright laws.

Sanctions/Remedies
Member States shall provide adequate legal protection and effective legal remedies. Again, the WPPT leaves it to Member States to decide what remedies are appropriate.

1.3.3. Further initiatives envisaged

The WIPO Expert Group on Copyright and Related Rights is currently preparing an additional instrument on the legal protection of the neighbouring rights of broadcasting organisations, because the broadcasting organisations as potential subject matter under neighbouring rights protection have not been considered within the framework of the WCT and WPPT.

Although there have been a number of concrete proposals, it is still too early to give any clear indications what the content of the instruments may be. It was generally agreed, however, that following the model of Article 11 WCT and Article 18 WPPT, a provision should be adopted to deal with the legal protection of technological measures when applied by broadcasting organisations in the context of the exercise of their neighbouring rights.

2. National regulations

2.1. Member States of the European Union

2.1.1.

Austria

Introduction

In Austria, there is no specific legislation on the legal protection of CA devices. Legal protection against those who commercially distribute pirated decoders is generally based on unfair competition law. No cases are known, however, where Article 1 Gesetz gegen den unlauteren Wettbewerb (UWG; unfair competition law) has been applied to acts of piracy against providers of *free CA services*.

Relevant general laws

Article 1 UWG has repeatedly been invoked by providers of pay-TV services as the basis for possible claims against acts of commercial distribution of pirate decoders. However, this is not effective against those who buy such devices.

Article 1 UWG provides for injunction against and compensation from those who perform acts of competition which do not comply with codes of fair behaviour. According to relevant jurisdiction, an act of competition requires the existence of real competition. The later is generally supposed to exist when enterprises address more or less the same consumers, whereas it is not necessary for actual competition to exist between the parties. Parity or similarity of goods or services offered is not required, just similarity of consumers.

Until now, however, Article 1 UWG has only been invoked in the context of pay-TV services. Thus, it remains to be seen whether courts also consider the sale of decoders etc. capable of decrypting services which use CA for non-remuneration reasons (but see below) as an offence against unfair competition law.

In addition, the provisions of copyright law may be applicable.

Case law
There has been a case concerning the sale of software which removes anti-copying protection from other computer software. In this context, CA was used for non-remuneration interests (i.e. copyright protection). The Court of Cassation decided that the sole unauthorised use of this kind of software by the consumer is an illegal or unfair act—in the sense of Article 1 UWG—committed by the vendor, who is the consumer's accomplice (Oberster Gerichtshof, 25 October 1988, WB1 1988/56).

Future legislation

There are plans to introduce legislation on the protection of CA devices in order to implement the Conditional Access Directive (CAD) into Austrian law (http://www.parlinkom.gv.at/archiv/XXI.pdf/ME/00/00/000018.pdf.). According to information from the Federal Ministry of Justice (the body responsible for implementation of the CAD), the aim is to strictly follow the provisions of the CAD. Thus, there are no plans to extend protection under Austrian law to providers of free CA broadcasting/IS services or to non-remuneration reasons to use CA. It has been indicated, however, that possibly the Austrian regulation will

be drafted in a way that allows it to be interpreted to also cover public broadcasters. Public broadcasting television is not provided against direct remuneration but against prior payment of a general licence fee. Thus, on the basis of a broad interpretation of ‘remuneration’, the new law may also prohibit unauthorised activities with intent to receive public broadcasts without having paid the license fee.

2.1.2.

Belgium

Introduction

In Belgium, there are two specific regulations on the legal protection of CA devices used by broadcasting services; however, there are no such provisions for IS services. The first provision applies to the French-speaking community (Décret of 27 July 1987 on broadcasting (M.B., 22 Augustus 1987)) and exclusively protects CA devices used by providers of pay-TV services, where this is done for remuneration reasons, whereas the provision applying to the Flemish community (Décret of 25 January 1995 on broadcasting (M.B., 30 May 1995): Besluit van de Vlaamse regering tot coordinatie van de decreten betreffende de radio-omroep en de televisie: Article 119) deals to some extent with the distribution of decoding devices irrespective of the reason CA serves and may apply also to free encrypted cable services.

Due to the recent constitutional and institutional reform in Belgium, broadcasting is now a matter of regional competence. There is therefore no specific federal legislation on piracy, nor is it clear if the federal government intend to implement new anti-piracy measures. However, if the regional legislation proves to be inadequate in the future, a law could be introduced at the federal level.

1. Articles 19, 43 Décret of 27 July 1987 on broadcasting

Details

Title: Articles 19, 43 Décret of 27 July 1987 on broadcasting (French-speaking community).
Date:1987
Source: M.B., Augustus 1987
Classification: Broadcasting law.
Remarks: Décret of 27 July 1987 applies to the French-speaking community, and Décret of 25 January applies to the Flemish sector. As far as the German-speaking community is concerned, there is no specific legislation.

Scope of protection

Services protected
Décret of 27 July 1987 covers television broadcasting, and possibly radio broadcasting. Whereas IS services are not covered.

Protection of free CA services
Décret of 27 July 1987 was reported to focus only on the protection of pay services.

Reasons protected
Décret of 27 July 1987 protects the remuneration and other economic interests of broadcasters.

Definitions
'Système d'access conditionnel' is defined as "l'ensemble des moyens matériels et logiciels utilisés soit par un ou des systèmes de gestion des abonnés, soit par le public lui-même dans le cadre d' une gestion locale de l'acceès aux services de radiodiffusion au seul public disposant des titres d'acceès requies" (Article 1 Section 19).

Unlawful activities
The Décret of 27 July 1987 primarily prohibits unauthorised reception and related activities, such as:
- the direct broadcasting of a decrypted programme to a third party without authorisation
- providing a recording of a decrypted programme to a third party without authorisation
- receiving a decrypted programme from a third party without authorisation.

No distinction is made between unauthorised activities for commercial purposes and those for private purposes.

2. Décret of 25 January 1995 on broadcasting

Details

Title: Décret of 25 January 1995 on broadcasting (Besluit van de Vlaamse regering tot coordinatie van de decreten betreffende de radio-omroep en de televisie: Article 119) (Flemish-speaking community).
Date: January 1995
Source: M.B., 30 May 1995
Classification: Broadcasting law

Scope of protection

Services protected
Article 119 Décret of 25 January 1995 on broadcasting protects only radio and television broadcasting. The regulation does not deal with the protection of IS services.

Protection of free CA services
Article 119 Décret of 25 January 1995 distinguishes between cable programmes and television programmes. In the former case, the programme signal does not need to be provided against remuneration in order to be protected, whereas in the latter case it does.

Reasons protected
Décret of 25 January 1995 does not distinguish between the different reasons the technology may serve.

Definitions
'Betaalomroep' is defined as "een omroep die aan elke ontvanger de gelegenheid biedt tegen extra betaling, bovenop de prijs van het kabelabonnement en/of kijk- en luistergeld, een selectie van programma's te ontvangen" (Article 119).

Unlawful activities
The Décret of 25 January 1995 focuses on such preparatory activities as:
- the manufacture, import, distribution, sale, rental, possession and installation of decoding devices
- the use of commercial communications
- the individual purchase or rental of decoding devices. (Whereas the specific provision applicable to the French-speaking community focuses on the unauthorised interception of signals).

No distinction is made between unauthorised activities for commercial purposes and those for private purposes.

3. Décret of 27 July 1987 + Décret of 25 January 1995

CA services and the interests of third parties
The relevant Belgium provisions do not take into account the possible interests of third parties which may be involved where CA techniques are used by service providers.

Sanctions/Remedies

Sanctions
Both decrees provide for fines (26 to 10.000 Belgian francs (Euro 0,63 – 248); these amounts are usually increased by a certain amount defined each year by law).

Administrative sanctions
In addition, under the Décret of 27 July 1987, a judge can order confiscation of any devices that were used to commit the offence.

Relevant general laws
On the federal level, the provisions of the general unfair competition law may be applicable to cases of circumvention.

Where existing legislation is not sufficient—at least in the French-speaking part of the country, where the distribution of decoding devices is not covered as well as it is on the federal level—case law has generally referred to unfair competition law in order to prohibit the distribution, manufacture or sale of circumventing devices, such as unauthorised decoders or decryption devices used to decrypt TV signals.

Furthermore, a bill on computer crime is pending in Belgium and its provisions may be applicable to the circumvention of access control systems. Article 550 bis Criminal Code (to be introduced by the bill) will prohibit unauthorised access to computer systems. A requirement for this prohibition will be that the person should have known that access was denied to him/her. In this case, the existence of a CA system could in itself be proof that the person was not allowed access.

Case law
No case law applying to the specific provisions on the legal protection of CA as described above is known. As far as case law does exist, decisions have been based on general laws,

particularly those on unfair competition. Reported decisions, however, deal exclusively with pay-TV providers which use CA devices for remuneration interests.

Future legislation

In Belgium it is apparently still under discussion who is responsible for the implementation of the CAD (Federal State or the Communities) and in which way the Directive might be given effect.

2.1.3.

Denmark

Introduction

In Denmark, there are specific provisions on the protection of broadcasting services based on CA techniques. Protection is granted irrespective of whether or not the service is offered against remuneration. However, no such legislation exists on the protection of (free or pay) IS services which use CA devices.

Details

Title: Danish Broadcasting Act, The Ministry of Culture's Consolidation Act No. 138, 19 February 1998
Date: February 1998
Source: http://www.kum.dk/
Classification: Broadcasting law

Scope of protection

Services protected
Article 75a Danish Broadcasting Act deals with the protection of the "contents of encoded radio or TV programmes".

IS services are not included. The regulation of IS services is the responsibility of a different ministry (Ministry of Research), which so far has not adopted any specific legislation on the protection of these services.

Protection of free CA services
Under Article of the 75a Danish Broadcasting Act, probably all encoded programmes are protected, including those provided for free (i.e. not against the payment of an additional fee).

Reasons protected
Since the Act does not mention specific reasons for implementing access control, probably all reasons to use CA are protected.

Unlawful activities
Only preparatory activities are prohibited. Furthermore, only activities carried out for commercial purposes are banned.

According to Article 75a Danish Broadcasting Act, it is prohibited as a commercial activity to:
- manufacture, import, sell, own or adapt decoders or other decoding equipment the purpose of which is to give unauthorised access to contents of an encoded radio or TV programme
- in addition, advertisements for or other forms of promoting such equipment are not permitted.

CA services and the interests of third parties
In Denmark, the provisions of Article 3b Television without Frontiers Directive have led to the implementation of a specific provision on encrypted programmes and the interests of third parties. The reason for this provision is the public's interest in receiving broadcasts of certain events of major importance to society. Accordingly, Article 75 Section 1 Danish Broadcasting Act states that the Ministry for Culture may lay down rules to the effect that television broadcasters may not exercise any exclusive rights to report on events of major importance to society in such a way that a substantial portion of the public is deprived of following such events on free, un-encrypted television. The same applies to television broadcasters subject to Danish jurisdiction as regards events which have been declared by other EU Member States to be of major importance to society (Article 75 Section 2).

The Minister for Culture may establish certain limitations regarding the exercise by television broadcasters of their exclusive rights to transmit such events. These limitations may allow other television broadcasters to broadcast short excerpts of the reported events, in order to secure for the public the "right to be kept informed" (Article 75 Section 3).

Sanctions/Remedies

Sanctions
Any person who deliberately or by gross negligence infringes Article 75a may be subject to a fine or imprisonment (mitigated imprisonment or a term of unmitigated imprisonment for up to 6 months) (Article 76a Danish Broadcasting Act).

Administrative sanctions
Confiscation of the pirate company's profit and pirate decoding equipment is possible according to the Penal Code. The law of administration of justice concerning search, inspection, confiscation, etc. applies to police investigations of pirate decoder cases.

Civil remedies
Ordinary liability laws apply. Rightholders in companies may initiate proceedings, either parallel to a criminal case or independently. It is possible to incur compensation liability, even if there is no punishable case (e.g. the breach was not deliberate, or it involved simple rather than gross contempt).

Case law
No case law applying to the provisions discussed above has been reported. Furthermore, no cases are known where providers of free CA services have claimed protection against pirate activities on the basis of general laws.

Future legislation

There are plans to draft additional legislation on the legal protection of CA services. The draft proposal is expected to deal exclusively with the protection of IS services. It is not felt necessary to adopt additional legislation with respect to broadcasting services which use CA devices (although there is some discussion concerning the prohibition of the private use of illicit devices).

The draft law covers only services that are "normally provided against payment". We have been informed, however, that this wording is not intended to exclude free CA services, but to

restrict application to services which have an own economic value (as opposed to e.g. private homepages or non-commercial information offers).

The draft law will prohibit preparatory activities performed for commercial purposes, such as the production, import, sale, possession, adaptation, etc. of decoders.

2.1.4.

Finland

Introduction

In Finland, there is specific legislation on the legal protection of CA techniques used for non-remuneration reasons. Although the regulation is part of the Finish telecommunication law, it is apparently also applicable to broadcasting services due to a broad definition of the term 'telecommunications'.

Details

Title: Section 25 of the Finish Telecommunications Market Act 396/1997
Date: Amendment April 1999
Source: http://www.mintc.fi/www/sivut/suomi/telemarkkina/telecom/norms/1997_396.htm
Classification: Telecommunications law

Scope of protection

Services protected
Television and radio broadcasting services (cable and satellite) are protected. IS services are not protected.

Protection of free CA services
Protection is granted irrespective of whether the service is provided against remuneration. Consequently, also free CA services are covered.

Reasons protected
No specific reasons are stated which the technology must serve in order to be protected. The main general interest objectives underlying the Telecommunications Market Act are to protect remuneration interests, to ensure security of communications, and to protect intellectual property rights and the economic interests of service providers.

Definitions
'Telecommunications network' means "the transmission systems which enable the transmission of messages between certain interconnection points either by wire, radio, optical or other electromagnetic means".

'Telecommunications service' means "a service the provision of which consists in part or as a whole of the transmission or routing of messages in a telecommunications network".

'Decoding system' means "any equipment, part of equipment or another system whose purpose is to decode the protective code effected through specific technical means from a message conveyed in the telecommunications network" (Article 4 Telecommunications Market Act).

Unlawful activities
According to Article 25 Telecommunications Market Act, the unlawful interception, possession, use, manufacture, import, marketing, sale, distribution, rental, installation, maintenance, replacement and sales promotion of a decoding system for a protective code is forbidden.

No distinction is made between unauthorised activities for commercial purposes and those for private purposes.

CA services and the interests of third parties
Under Article 25, it is possible to obtain permission from the Telecommunications Administration Centre (TAC) to use a decoding system which normally could also be used to circumvent the encrypted offers of other service providers. TAC is entitled to react to exceptional situations.

It was not reported, however, whether the provision has already been applied.

Sanctions/Remedies

Sanctions
Article 45 Telecommunications Market Act states that anyone who wilfully possesses, manufactures, uses, imports or markets a decoding system or promotes its sales in violation of Article 25 shall—if a more severe penalty is not provided for elsewhere in the law—be fined for violating the provisions on telecommunications operations to a fine or imprisonment up to 6 months.

Administrative sanctions
According to Article 42, TAC or the responsible ministry may impose a conditional monetary fine or administrative sanction (i.e. to partly or fully discontinue the operation). In addition, any economic benefit accruing to the person who committed the crime or to the person on whose behalf the crime was committed can be subject to seizure according to the rules of the Penal Code. A decoding system used to commit a crime shall be forfeited to the State except in extremely mitigating circumstances (Article 46 Telecommunications Market Act).

Civil remedies
It is unclear to what degree it is possible to initiate civil proceedings. In Finland, it is generally possible to apply for damages during criminal proceedings. Any party concerned (e.g. a copyright holder) can bring a criminal case against a person who used an illegal decoder. In practice, it seems possible to initiate civil proceedings against professionals, but not against persons who act for private viewing purposes.

Enforcement
The Telecommunications Market Act includes some detailed regulations on means and procedures of enforcing the provisions on decoding devices. According to Article 39, an inspector appointed by TAC[95] shall supervise the import, marketing and sales promotion of telecommunications terminal equipment and decoding systems.

If an inspector discovers evidence of a possible violation of the Act, he has the right to gain access to a place where telecommunications terminal equipment or a decoding system is

[95] "The Telecommunications Administration Centre shall control compliance with this Act and with the provisions and orders issued thereunder" (Article 35 Telecommunications Market Act).

located or where such is suspected on reasonable grounds to be located. TAC is entitled to executory assistance from the police, the customs authorities and the Frontier Guard.

If there is probable cause to suspect that Article 25 (decoding devices) has been violated, the inspector has the right to remove the equipment for inspection and forbid the marketing or transfer of the equipment or system during the inspection to be carried out.

At the request of the inspector, anyone marketing telecommunications terminal equipment must provide the inspector with information on the technical specifications and conveyance of the equipment .

General legislation
Section 7 Radiolag (law on radio communications) protects the secrecy of signals and may be applicable where CA systems are used to protect them. According to this provision, it is prohibited to record, disclose or make use of the contents or the knowledge of the existence of radio communication not intended for reception by the person who receives the service. It is also prohibited to possess equipment intended to remove protection, achieved by means of a special technical system, from such radio communication, without permission from TAC. Anyone who violates these provision may be ordered by TAC to amend his/her fault or neglect, and TAC may impose a conditional fine.

Case law
No case law applying to the provisions discussed above has been reported.

Future legislation

There are plans to draft additional legislation to protect CA services and implement the CAD.

According to information from the Ministry of Transport and Telecommunication (which is responsible for the implementation of the CAD), planned legislation will protect not only television and radio broadcasting services, but also IS services. The new law—which is still being drafted—will transfer the existing provisions on CA to a separate act. As far as the protection of free CA services is concerned, it is planned to narrow the scope of the existing legislation (described above) by excluding free CA services from its scope. This decision was explained by reference to the CAD, which does not include free CA services.

It is expected that the draft will be presented to parliament within a few weeks.[96]

[96] State: 07.03.2000

2.1.5.

France

Introduction

France was one of the first EU Member States to introduce specific legislation on the legal protection of CA services. The relevant provision was originally in Article of the 429 French Penal Code (Loi No. 87-520 of 10 July 1987), but has now been implemented in Article of the 79 French Audiovisual Law. The provision focuses exclusively on the protection of pay CA services.

Details

Title: Article 268 Loi No. 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du noveau code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cetter entrée en vigueur
Date: December 1992
Source: Journal Officiel No. 298 du 23 décembre 1992
Classification: Penal law
Remarks: Modifies Article 79 Loi No. 86-1067 of 30 September 1996 on the freedom of communication

Scope of protection

Services protected
Article 268 Act No. 92-1336 (Article 79 Loi No. 86-1067) protects audiovisual services, i.e. radio, broadcasting and probably also IS services.

Protection of free CA services
Programmes fall under the scope of Article 268 Loi No. 92-1336 (Article 79 Loi No. 86-1067) if they have been restricted to a limited audience which has obtained access by paying a fee to the service provider. In other words, only pay CA service providers are subject to protection.

Reasons protected
The law does not distinguish between the different reasons CA devices may serve, as long as the service is distributed by a pay CA service provider.

Unlawful activities
Prohibited activities are manufacture, importation with intent to sell or rent, offer to sell, storage with intent to sell, sale or installation of equipment, appliances or instruments designed wholly or partly to fraudulently receive protected broadcast programmes (Article 79 Section 1). It is also prohibited to order, design, organise or distribute advertising material which promotes such equipment (Article 79 Section 2).

In addition, private possession or acquisition of such equipment, appliances or instruments with intent to use is punishable (Article 79 Section 4).

Sanctions/Remedies

Sanctions
Violations of Article 79 can be punished by imprisonment up to two years and the imposition of fines up to FF 200.000 (Euro 30490).

Administrative sanctions
In addition, the court may order the confiscation of equipment, appliances, instruments and advertising material (Article 79 Sections 5, 6).

Case law
No case law dealing with the circumvention of free CA services which use CA devices has been reported.

Future legislation

Presently, two draft laws concerning implementation of the CAD are being discussed (see www.Internet.gouv.fr). The proposals concern both broadcasting and information services. Currently, however, there are no plans to exceed the provisions of the CAD by including free-service providers which use CA devices.

2.1.6.

Germany

Introduction

In Germany, there is no specific legislation on the legal protection of CA services. However, there are plans to adopt such legislation in order to implement the CAD.

Relevant general laws

Cases of circumvention of CA devices used for non-remuneration reasons could be dealt with under general laws, particularly the unfair competition law (Articles 1, 17 UWG; Industrial espionage) and the penal law (Article 202a Criminal Code; Data theft). However, some penal provisions which probably could be applied for directly remunerated CA services (e.g. 263a Criminal Code (Computer fraud); 265a Criminal Code (Leistungserschleichung)) do not seem suitable for situations in which CA devices are used by providers of free CA services, since they protect direct financial gains or direct payment interests.

Case law
No case law dealing with free CA services as victims of pirate activities has been reported. However, one case law concerned multifunctional decoders which are also capable of circumventing non-directly remunerated services (Firma Teleclub GmbH v. Firma Manfred Haas GmbH, Oberlandesgericht München (Court of Appeal), 19 March 1992, 29 U 4370/91). During the proceedings, the defendant claimed that his devices were multifunctional and not specifically designed to circumvent the CA devices of the plaintiff. The defendant had been selling devices which could be used for a variety of reasons, including to gain access to the CA-based pay TV service of the plaintiff. The defendant claimed that his decoders were not specifically designed to enable unauthorised access to the plaintiff's services. However, the court did not accept this argument and convicted the defendant of an offence under Article 1 UWG.

Future legislation

Currently, new legislation on the legal protection of CA devices is being drafted, in order to implement the CAD into German law. According to information from the responsible ministry, however, at the moment there are no plans to exceed the scope of the Directive by extending protection to providers of free CA services.

2.1.7.

Greece

Introduction

In Greece, there is currently no specific legislation on the legal protection of CA services.

Relevant general laws

In a circumvention situation, a variety of general laws may apply, such as civil and penal law and the general law on data protection, telecommunication and broadcasting, which may also be invoked by providers of free CA services.

Case law
No relevant case law has been reported. There have been some out of court settlements between subscriber television service providers and consumers who had illegally used decoder equipment to access their services. These cases, however, dealt with acts of circumvention carried out with intent to avoid paying requested fees.

Procedural provisions
The concession contract to be signed in mid-December between the Minister of Press and Mass Media and the multi-choice service providers of digital TV pay-per-view services (NOVA) is reported to embody specific regulations on procedures for out of court settlement in the case of piracy activities. Further details are unknown at the time of writing, since the agreement has not yet been published.

Future legislation

There are plans to implement the CAD into national law. It was not yet reported how Greece will give effect to the CA Directive.

2.1.8.

Ireland

Introduction

In 1990, Ireland adopted specific provisions on the legal protection of broadcasting services against pirate activities in its Broadcasting Act. Article 9 of the Act focuses primarily on the unauthorised interception of broadcasting irrespective of whether or not programmes are encrypted. It is very questionable whether the provision could be interpreted in a sense also to cover encrypted free CA services.

Details

Name: Broadcasting Act 1990
Date: July 1990
Source: http://www.ucc.ie/ucc/depts/law/irishlaw/
Classification: Broadcasting law
Remarks: Article 16 Broadcasting Act includes a provision empowering the Minister of Communication to extend protection to encrypted, wireless transmitted pay-TV services. Whereas it is not clear whether this also applies to free encrypted services.

Scope of protection

Services protected
Article 9 of the Irish Broadcasting Act specifies two groups of beneficiaries: licensees and service providers. The former are considered broadcasting services, included encrypted services, in the sense of the Wired Broadcast Relay Licence Regulations 1974 or of the Wireless Telegraphy (Television Programme Retransmission) Regulations 1989, which are primarily cable broadcasting and MMDS services.

Article 16 enables the provisions to be extended to pay-services on any wireless apparatus by the making of an order (in the sense of "any class of service transmitted by wireless telegraphy intended by the service provider to be received only by persons paying a fee to the service provider"). Up to now, an order under this section has not yet been made. From Article 16, however, one could also conclude that, until now, access controlled service do not fall under Article 9 unless an adequate order has not been made.

Protection of free CA services
In its present form, the Irish Broadcasting Act 1990 possibly could be understood to also protect access controlled free CA services which are transmitted via cable or MMDS systems.

Reasons protected
Article 9 of the Irish Broadcasting Act does not directly deal with the protection of technological measures but rather with the unauthorised interception of services. Consequently, the Act does not distinguish between the different reasons CA devices may serve.

Definitions
'Interception' means in relation to a service, "to receive, view, listen to, record by any means or acquire the substance or purport of the service or part thereof supplied by a licensee or service provider without the agreement of the licensee or service provider".

'Encrypted programme transmission' means a transmission in a form "whereby the aural or visual characteristics (or both) are modified or altered for the purpose of preventing the unauthorised reception of such transmission by persons without authorised equipment which is designed to eliminate the effects of such modification or alteration".

Unlawful activities
Irish broadcasting law does not directly address the unauthorised circumvention of technological measures, but rather, in more general terms, the unauthorised interception of services. It is not even necessary that services are encrypted in order to deserve protection. Prohibited are acts of unauthorised interception of services as well as preparatory activities for such acts. In this context, interception is understood in a broad sense not only as unauthorised reception but also as forms of exploitation of programmes, such as recording or acquiring the substance or purport of the service.

In detail, prohibited are the (individual) act of unauthorised interception as well as preparatory or auxiliary activities. In particular, it is unlawful to:
- intercept the service
- suffer or permit or do any other thing that enables such interception by any person
- possess, manufacture, assemble, import, supply or offer to supply any equipment which is designed or adapted to be used for the purpose of enabling such interception by any person, or
- publish information with the intention of assisting or enabling any person to intercept a service
- knowingly install or attempt to install or maintain any equipment which is capable of being used or designed or adapted to be used for the purpose of enabling such interception by any person. Furthermore, it is prohibited to
- wilfully damage or attempt to damage a system or part of a system operated by a licensee or service provider.

It is not important whether activities are carried out for commercial or private purposes.

CA services and the interests of third parties
The Minister for Communications may authorise one of his officers to perform acts as described above, probably for such reasons of public interest as public security.

Enforcement
The regulation contains quite extensive provisions concerning enforcement. Courts can provide the police with search warrants in order that they may enter, by force if necessary, and search places where illicit equipment is suspected to be present. Any person impeding the work of the police shall be guilty of an offence.

Procedural provisions
The Broadcasting Act contains specific provisions concerning the onus of proof, in order to facilitate law enforcement in the courts. Firstly, the owner of illicit devices is considered an accessory unless he/she can prove that he/she did not knowingly permit an offence. Secondly,

the defendant bears the onus of proof in demonstrating the existence of an authorisation to intercept a service.

Sanctions/Remedies

Sanctions
Any person found guilty of an offence can be liable to a fine not exceeding Pounds 1000 (Euro 1270) or imprisonment not exceeding three months in case of summary conviction, and Pounds 20.000 (Euro 25395) / 2 years in case of conviction on indictment.

Administrative sanctions
Courts may order the forfeiture of equipment.

Civil remedies
Licensees or service providers who have suffered, suffer or may suffer damages may apply for an order of the High Court of Circuit to restrain the defendant from carrying on or attempting to carry on the infringing activity as well as for damages or an account of profit.

Case law
No case law has been reported on the application of the reported provisions on providers of free CA services or CA devices used for non-remuneration reasons.

Future legislation

The responsible department is currently examining ways in which the CA Directive might be given effect. One option is to make an order under Section 16 of the Broadcasting Act, 1990. It is not yet clear whether Ireland will exceed the scope of the CA Directive by extending protection to free CA services provided on the basis of access control – the issue is still under discussion.

As to the use of CA and third parties interests possibly concerned, the draft proposal for a new Irish Broadcasting Bill 1999 contains certain provision on Electronic Program Guides (EPGs). The person who makes available EPGs, may be obliged to ensure that EPGs may easily be used by a member of the public to access information in relation to the schedules of programme material. EPGs shall not be designed in such a way as to result in a user of the guide experiencing difficulty in accessing the programme material supplied (Section 12 (5), (6)). Furthermore, the preparation of guidelines is foreseen with respect to the format in which the information in relation to schedules of programme material provided by electronic programme guides may be presented (Section 13).

The draft Broadcasting Act 1999 also includes a provision on the further free accessibility of the national public television and broadcasting service. It apparently shall have the character of a public service and continues to be a free-to-air service and be made available, insofar as it is reasonably practicable, to the whole community on the island of Ireland (Section 24 (1)).

2.1.9.

Italy

Introduction

Italy has already adopted several specific laws on the legal protection of CA services, which protect access controlled broadcasting services probably irrespective of whether they are provided against direct remuneration or not. However, the existing legislation focuses on the protection of services which are provided against remuneration.

Details

Title: Article 11-1 bis Law No. 422
Date: 1993
Source: Gazetta Ufficiale della Republica Italiana, 5 November 1993
Classification: Broadcasting law

Scope of protection

Services protected
Only television broadcasting services are protected; radio broadcasting and IS services are not protected.

Free CA services protected
The law covers encoded broadcasting services in general, probably without distinguishing between pay-TV and other services. Thus, providers of free CA services could also claim protection under this provision.

Reasons protected
Protection is not conditional on the reason the technology serve. The underlying principles under the provision have been reported to cover remuneration interests, protection of intellectual property rights, economic interests as well as other interests such as the protection of minors.

Unlawful activities
Prohibited activities are:
- the duplication of encoded transmissions (i.e. signal theft)
- the importation, distribution, sale, possession for commercial purposes, rental of unauthorised means intended solely to allow or to facilitate arbitrary removal or circumvention of devices applied for the protection of encoded transmissions.

Sanctions/Remedies

Sanctions
Offences can be punished by imprisonment and/or monetary fines up to ITL 6.000.000 (Euro 3099).

Civil remedies
Aggrieved parties may bring a civil action.

Case law
No specific case law on the circumvention of free CA services has been reported. However, there has been a case dealing with multi-decoders, i.e. the CMR case. CMR was manufacturing illegal decoders and devices capable of 'cloning' legal decoders. CMR claimed that their decoding devices were not intended to provide unauthorised access to Télépiu, but to a free Dutch satellite service which had been encrypted for copyright reasons. The defendants claimed that their devices were programmed to decrypt the programmes of the Dutch pay-TV channels, which were transmitting their analogue signal via satellite using the same decoding system utilised by Tele+ (i.e. Irdeto). According to CMR, it was mere coincidence that Tele+ could be decoded using their device. The case was never finally decided. After Télépiu appealed to the public prosecutor in Rome, the case was turned down due to lack of evidence.

Future legislation

There are plans to adopt additional legislation on the protection of CA in order to implement the provisions of the CAD into Italian law. This regulation is the Draft Regulation of the Autorita per le Garanzie nele Comunicazioni on the definition of a common decoder standard (Schema concernente la determinazione degli standard del decodificatori e le norme per la ricezione del programmi televisivi ad accesso condizionato, non definitivo; broadcasting law).

Probably, the provision will protect only broadcasting services and services provided against payment ('servizi televisivi numerici a pagamento'). The provision prohibits not only the distribution, sale, rental and possession of decoding devices, but also their manufacture.

To a certain degree, the draft also takes the interests of third parties into account. In particular, the provisions seem to exceed what is regulated in the Standards Directive. According to Article 2 of the draft, the providers of access control who provide digital television programmes on their own shall guarantee that it is possible to receive with the same decoder all other broadcasting services which are based on access control and provided by other service providers (Article 2 of the proposal).

Providers of CA devices may be obliged to provide consumers with sufficient information concerning which broadcasting services (also those from competing providers) can and which cannot be received via a particular device (e.g. a set-top box). In addition, devices must be equipped with a programming help function enabling the user to request information about the distributor of a service and the content of a specific digital programme (Article 5 of the draft).

The draft also includes specific provisions on EPGs and APIs. EPGs must contain correct information on all offers (also those from competing service providers) and be open to all operators on fair, reasonable conditions. In addition, operators of CA devices must ensure that the APIs they have implemented are open to all service providers. Moreover, providers of CA devices are obliged to assist other service providers with the implementation of a particular API.

2.1.10.

Luxembourg

Introduction

In Luxembourg, there is no specific legislation on the legal protection of CA devices. To a certain extent, this is because at the moment there are no encrypted services specifically intended for the population of Luxembourg. Most programmes are supplied by neighbouring countries.

Relevant general laws

No cases have been reported in which a court had to judge a case concerning the circumvention of (free or pay) CA services. If such a case were to arise, the protection of CA services could probably be found in general laws, particularly the Civil and the Penal Code. In the Civil Code, the obvious provision would be Article 1382. This is a general tort law provision, i.e. an obligation to compensate for any harm done to another person. Civil proceedings eventually may only be brought against persons who act for commercial purposes.

In the penal law, reference can be made to the law of July 15, 1993 (La Loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique), the objective of which is to reinforce the fight against economic crime and information fraud and provides a modification of the penal law.

Future legislation

Luxembourg is currently preparing to implement the provisions of the CAD into national law. At the time of writing, this draft law has not been published. It is expected that the new law will be presented to parliament before the summer break 2000.

As far as can be judged, the government intends to transform the Directive in its present form without extending its scope to free CA services.

2.1.11.

Portugal

Introduction

In Portugal, there are no specific regulations on the legal protection of any CA devices, irrespective of what reason they serve.

Relevant general laws

Two laws relevant to the protection of personal data may be applicable here:
Law No. 76/98 of 28 October (implementation of the 95/46/EC Directive, 24 October 1995), and
Law No. 69/98 of 28 October (implementation of the 97/66/EC Directive, 15 December 1997).

Future legislation

It has not been reported yet if and how Portugal will give effect to the CA Directive.

2.1.12.

Spain

Introduction

There is no specific legislation on the legal protection of CA-based (free or pay) services. However, there are plans to introduce legislation in order to implement the CAD. When implementing the Directive into national law, Spain plans to adhere to its precise wording. Thus, free CA services which use CA will not be protected.

Relevant general laws

In case of the unauthorised circumvention of free CA services which use CA, the provisions of the Spanish Civil Code and Penal Code (protection of property) may be applicable. The Industrial and Intellectual Property Law may also provide for some protection.

Case law
However, no cases where these provisions were applied during legal proceedings which were initialised by providers of access controlled free CA services are known.

Future legislation

Spain is drafting a new law in order to implement the CAD into Spanish law. The regulation is expected to focus exclusively on the protection of CA in a situation where access control is applied to serve the remuneration interests of service providers; it will not provide for the legal protection of access control mechanisms which serve other interests. The issue of protecting free CA services which use CA devices, apparently, has not yet been discussed in Spain. The proposed new law exceeds the CAD in so far as there are plans to prohibit the possession of decoding devices for personal purposes outside the home (possession inside the home will remain lawful).

2.1.13.

Sweden

Introduction

In Sweden, only legislation on the legal protection of encrypted pay radio and television broadcasting services exists. The relevant provisions were implemented into Swedish penal law in December 1993.

Details

Title: Lag (1993:1367) om förbud beträffende viss avkodningsutrustning
Date: December 1993
Source: SFS Nr. 1993: 1367
Classification: Criminal Law (separate law)

Scope of protection

Services protected
Protected are radio and television broadcasting services.

Protection of free CA services
Services are protected only when provided against remuneration.

Reasons protected
The law was reported to focus on the protection of remuneration reasons, security and intellectual property rights. Is has been argued that it is also an overall purpose of the Act to protect the economic interests of service providers in general, i.e. also those of providers of free CA services which have a certain economic value. However, this interpretation cannot be explicitly concluded from the regulation. Furthermore, particularly in the field of criminal law, generally only an interpretation which is as literal as possible is considered appropriate.

Unlawful activities
The manufacture, sale, rental, installation and maintenance of decoding devices for commercial purposes are prohibited.

CA services and the interests of third parties
The Swedish regulation does not take into account the interests of third parties.

Sanctions/Remedies

Sanctions
Violations can be sanctioned with a monetary fine and/or prison sentence up to 6 months,.

Administrative Sanctions
Courts may order seizure of any object of offence (or value thereof) and of profit, if not obviously unreasonable. Seizure of means is possible for reasons of prevention or other specific reasons.

Civil remedies
Civil proceedings can be held parallel to a criminal case, or separate. There is a right to claim damages, which have been proven. It is unclear who may start proceedings.

Relevant general laws
The Swedish Act on Copyright in Literary and Artistic Works and the Tort Liability Act may be applicable.

Case law
No cases have been reported in which providers of free CA services claimed legal protection against piracy under general laws. The same applies to the specific provisions on the protection of pay services.

Future legislation

There are plans to adopt a new Swedish Conditional Access Act (Regeringens proposition 1999/2000: 49 Utökat skydd för kodade tjänster). The proposed act will be in the field of criminal law. The recent proposal, however, does not take into consideration the legal protection of CA devices where they are used by free CA services or for non-remuneration reasons. The proposed act concentrates on protecting the remuneration interests of the providers of pay services. Unlike the previous law, this act will also take into account IS services and will extend the catalogue of unlawful activities to cover the activities protected under the CAD (except the use of commercial communications to promote decoding devices).

Under the proposed bill, parties who deliberately breach the provisions of the new Conditional Access Act will be obliged to pay compensation for the use of the service as well as for the additional economic damage the violation has led to. Third parties (such as rightholders) may claim compensation on the grounds of the Swedish Act on Copyright in Literary and Artistic Works, as well as on the Tort Liability Act.

2.1.14.

The Netherlands

Introduction

In the Netherlands, specific provisions on the legal protection of CA services are embodied in the Penal Code, primarily in the Law on Computer Criminality (Wet Computercriminaliteit), which was drafted in order to adapt the existing provisions of the Penal Code to the electronic environment.

Although protection is not conditional on whether a service is offered against remuneration, the provision applies only to situations in which circumvention has occurred with intent to avoid paying the full price for the service.

The Dutch provision is an example of a national regulation in which the term 'remuneration' could be interpreted in a broader sense so as to also cover non-direct remuneration interests, such as the provision of general license fees and, by doing so, also to address public broadcasters.

Details

Title: Article 48 and 326c Wetboek van Strafrecht (WvS; Penal Code)
Date: December 1992
Source: Stb. 1993, 33 (Law on Computer Criminality)
ClaHYPERLINKssification: Criminal law
Remarks: The provision originates from Article 50.3 Wet op de Telecommunicatievoorzieningen (Law on Telecommunications)

Scope of protection

Services protected
Article 326c WvS protects telecommunication services (including broadcasting) and IS services. The provision covers telecommunications services in general, since it does not explicitly state that a service must use encryption or another form of access control in order to be protected.

Protection of free CA services
Protection is not explicitly conditional on whether the signal is provided against remuneration in the sense as used in this study. From the wording of the provision it can be concluded that the service should require at least some form of remuneration from the audience in order to be worthy of protection (which is not the case with e.g. a private homepage or a voluntary transmission). Thus, the provision could also cover cases in which a person wants to receive the programmes of a public broadcaster without having to pay the general license fee. However, it is questionable whether the provision applies to broadcasters financed by commercial advertisements where no financial contribution is necessary in order to receive the programme.

It should be noted, however, that due to the recent amendment of the Dutch Broadcasting Law (Media Wet), from the beginning of the year 2000, license fees will no longer be charged. This may mean that public broadcasters will no longer be able to claim protection under the provisions of Article 326 c WvS.

Reasons protected
Article 326c WvS protects the remuneration interests of the service provider in a broader sense.

Unlawful activities
It is prohibited to make use, through a technical intervention or with the help of false signals, of a service which is offered to the public by way of telecommunications, with intent not to pay the full price (Article 326c Section 1). In other words, protection is conditional on the existence of malicious intent not to pay for the service.

The wording of Section 1 is quite broad. It covers not only the unauthorised use of illicit decoding devices (irrespective of whether this is software or hardware, passwords, keys or any other information), but also all sorts of technical means, such as technical reception devices. This is because not only encrypted signals but also unencrypted signals are subject to protection.

It should be noted that Section 1 addresses not the use of illicit devices or unauthorised access itself, but the use of a service with intent not to pay the remuneration due.

Under Article 48 WvS, accessories to a concrete offence (such as those who produce decoding devices, irrespective of whether such production was for commercial purposes) may be punishable.

Section 2 Article 326c focuses on the manufacture of illicit decoders in general. According to Section 2, it is unlawful to deliberately offer in public for distribution, have available with intent to distribute or import into the Netherlands, or manufacture or store for financial gain, an object or data apparently intended for violating the provisions of Section 1.

CA services and the interests of third parties
There are no plans to implement into Dutch law a specific provision to directly take into account the interests of third parties as far as access controlled services are concerned. Article 2 Section 1 Telecommunicatie Wet (Telecommunication Law), however, stipulates that those who want to offer a CA device must register. This gives OPTA (Onafhankelijke Post- en Telecommunicatie Autoriteit – Independ Authority for Post and Telecommunications) the possibility to check whether the offered service complies with existing laws. OPTA's main task is to supervise the provisions which implement the Standard Directive into Dutch law.

Sanctions/Remedies

Sanctions
Offences against the provisions of Article 326c WvS can be punished with prison sentences up to 3 years and/or monetary fines up to Dfl 100.000 (Euro 45378). If an offence was performed professionally the judge may impose a longer prison sentence or a higher fine.

Administrative sanctions
In addition, a court may order the seizure of goods, publication of the sentence and expulsion from the occupational field in which the offence took place. Profits can also be seized.

Relevant general laws
Additional provisions which may be applicable to circumventing activities are embodied in Article 161 sexies (unauthorised circumvention of electronic protection measures). In addition, civil proceedings can be brought on the basis of Article 6:126 Burgerlijk Wetboek (Civil Code), which deals with uncompetitive behaviour.

Case law
No cases have been reported on the circumvention of free CA services which use CA or the circumvention of CA used for non-remuneration reasons.

Future legislation

There are presently no plans to draft additional legislation on the legal protection of CA, since it is claimed that the existing provisions satisfy the requirements of the CAD.

2.1.15.

United Kingdom

Introduction

In the UK, specific legislation on the legal protection of CA techniques is embodied in Articles 297-299 Copyright, Designs and Patents Act 1988 (CDPA) as amended by Article 140 Broadcasting Act 1996 and Article 179 Broadcasting Act 1990. The law, possibly, could be interpreted to also cover public broadcasting services using CA devices.

Details

Title: Sections 297A and 298 CDPA as amended by the 1990 and the 1996 Broadcasting Act
Date: 1996
Classification: Copyright act
Remarks: Under UK copyright law, broadcasters are considered first owners of copyright in the content of the programmes

Scope of protection

Services protected
The Act protects television and radio broadcasting services, as well as cable and probably IS services in as far as these services are directed at the public. This is due to a broad definition of broadcasting as "any transmission … of visual images, sounds or other information" (Section 6 (1b) CDPA).

Protection of free CA services
Under the Act, only unauthorised circumvention with the intent "to avoid payment of any charge" is prohibited.

In this context, 'unauthorised' in relation to a decoder means "to enable encrypted transmissions to be viewed in decoded form without payment of the fee (however imposed) the person making the transmission, or on whose behalf it is made, charges for viewing these transmissions, or viewing any service of which they form part" (Section 179 Broadcasting Act 1990, which was inserted as Section 297A in the CDPA).

Consequently, this provision could be interpreted in a broad sense to include the fraudulent reception of public, fee-based, broadcasting programmes (Section 297 CDPA).

Reasons protected
Under UK law, two reasons to use CA are protected, i.e. to ensure remuneration interests and to protect copyrights.

Unlawful activities
Under Sections 297A and 298 CDPA, the commercial manufacture, importation and commercial promotion and advertising of unauthorised decoders is unlawful. The same applies to sale and hire, as well as to offering and exposing for sale and hire.

While personal possession per se is not unlawful in the UK, unauthorised reception of an encrypted service by an individual with the intent to avoid payment is an offence (Section 297 CDPA).

Sanctions/Remedies

Sanctions
Violations of the Act are subject to criminal penalties (Section 297A CDPA), i.e. fines up to Pound 5000 and/or imprisonment. In case of innocent infringements, courts may reduce the hight/lenght of sanctions.

Administrative sanctions
General UK legislation enables courts to order the confiscation of the proceeds of crime if the criminal offence was a serious one.

Civil remedies
In addition, civil remedies are available; these are the same as those which apply in the case of copyright infringements, and provide for damages, injunctions and compensation for loss of profit.

The UK law grants the right to initiate proceedings to any person who is responsible for the content of a programme that has been received without authorisation or who transmits the broadcast while being at least responsible for the content. This means that any service provider—even if it did not participate in the process of making a programme—may claim rights.

Procedural provision
The UK offers protection against the unauthorised reception of services transmitted from a state other than the UK, under the condition that the foreign service provider obtains an order from the Ministry of National Heritage (Section 299).

Case law
No case law dealing with the unauthorised circumvention of programmes of providers of free CA services (e.g. public broadcasters) has been reported.

Future legislation

There are plans to adopt additional legislation on the legal protection of CA devices. The Conditional Access (Unauthorised Decoders) Regulation 2000 (which will come into force on 28 May 2000) extends the list of unlawful activities under the CDPA to include possession, installation, maintenance or replacement for commercial purposes of an illicit device, and will also require an extension of the protection afforded to include services transmitted from any place within the EU.

Also under the new Conditional Access Regulation 2000, the term ‘unauthorised’ in relation to decoders means “the decoder will enable an encrypted transmission to be accessed in an intelligible form *without payment of the fee (however imposed)* which the person making the transmission, or on whose behalf it is made, charges for accessing the transmission, or any

service of which it forms part, or that the decoder enables the circumvention of any CA technology related to the transmission or service".

The term 'however imposed' indicates that the payment requirement in this context has to be interpreted in a broad sense, thus probably also covering public broadcasting programmes which are provided against payment of a general license fee.

In the explanatory note to the draft regulation, it is furthermore mentioned that extending the CAD to cover non-directly remunerated services was discussed. Also during the drafting process of the new regulation, the issue of free CA services which use CA was paid attention to. It was decided, however, to adhere for the time being to the exact wording of the Directive.

2.2. Non-European Countries

2.2.1.

Australia

Introduction

In Australia, there are no specific provisions on the legal protection of CA services. However, such legislation is planned. The Copyright Amendment (Digital Agenda) Bill 1999—which was introduced into the House of Representatives on 2 September 1999—seeks to establish a number of very detailed provisions on the legal protection of CA devices. The proposed provisions can be subdivided into the protection of technological measures that serve copyright reasons and—similar to the UK approach—the protection of technological measures used by broadcasters for remuneration reasons.[97] The latter provisions focus exclusively on the protection of directly remunerated broadcasting services.

Details

Title: Articles 10(1), 116(1), 116A, D, 132 (5B-L), 132 (6B-C), 135AL, 135AN, 135AS, AT, AU of the Copyright Amendment (Digital Agenda) Bill 1999, No.[ ],1999—A Bill for an Act to amend the Copyright Act 1968 and for related purposes
Date: Presented to the House of Parliament in September 1999
Classification: Copyright law
Remarks: At the time of writing, the bill is still pending

1. Article 135 AL Copyright Amendment (Digital Agenda) Bill 1999

Scope of protection

Services protected
Under Article 135AL subsq., subscription broadcasters are protected who make an encoded television or radio broadcast.

Protection of free CA services
Free broadcasts provided on the basis of the same CA technology are, per definition, not considered encoded broadcasts in the sense of Article 135 AL and, thus, not included.

Reasons protected
Article 135(AS, AT, AU) does not distinguish between the different reasons a technological measure may serve, as long as the technology is used by a subscription broadcaster, i.e. pay-TV broadcaster.

Definitions
A 'broadcast decoding device' is defined as "a device (including a computer program) that is designed or adapted to enable a person to gain access to an encoded broadcast without the

[97] In addition, the Television Broadcasting Services (Digital Conversion) Act 1998 schedule 4, which is yet to come into force, includes provisions on CA systems. However, since these provisions deal exclusively with standardisation problems, they will be not discussed in this study.

authorisation of the subscription broadcaster by circumventing, or facilitating the circumvention of, the technical means or arrangements that protect access in an intelligible form to the broadcast" (Article 135 AL).

'Encoded broadcast' is in this context defined as "a broadcast a) delivered by a broadcasting service that is made available only to persons who have the prior authorisation of the subscription broadcaster and only on payment by such persons of subscription fees; and b) access to which in an intelligible form is protected by a technical measure or arrangement (including a computer program)" (Article 135 AL).

'Subscription broadcaster' means "a person who makes an encoded broadcast" (Article 135 AL).

2. Article 116 A Copyright Amendment (Digital Agenda) Bill 1999

Scope of protection

Services protected
Article 116A addresses works that are subject to protection by an "effective technological measure".

Protection of free CA services
Free CA services (probably irrespective of those are broadcasting or IS services) may be protected where they use technological measures to protect own copyrights in the content of a service. A remuneration interest is not necessary to be protection worthy under Article 116 A.

Reasons protected
Article 116A protects only copyright reasons.

Definitions
'Circumventing device' is "a device (including a computer program) that has only a limited commercially significant purpose or use, or no such purpose or use other than the circumvention, or facilitating the circumvention, of an effective technological protection measure (i.e. either limited commercially significant purpose or specifically directed upon circumvention of protection)" (Article 4 Subsection 10 (1)).

'Circumvention service' means "a service, the performance of which has only a limited commercially significant purpose, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of an effective technological protection measure" (Article 5 Subsection 10 (1)).

'Effective technological measure' means "a device or product, or a component incorporated into a process, that is designed to prevent or inhibit the infringement of copyright subsisting in a work or other subject matter if, in the ordinary course of its operation, access to the work or other subject matter protected by measures is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject matter) with the authority of the owner of licensee of the copyright in a work or other subject matter" (Article 8 Subsection 10 (1)).

3. Article 135 AL + Article 116 A

Unlawful activities
The catalogue of unlawful activities is similar for both categories of devices (protecting copyright/remuneration reasons) and focuses exclusively on preparatory activities to circumvent technological measures for commercial purposes.

The regulations on broadcasters clearly focus on the protection of CA devices, whereas the definition of technological measures to protect copyrights is broader and not specifically focussed on CA techniques. However, under Article 116A protection is conditional on the effectiveness of a device. In this context, particularly CA techniques are considered to be effective (see definition above) and thus, probably fall under Article 116 A.

It is prohibited to:
- make a circumvention device capable of circumventing or facilitating circumvention
- sell or let for hire
- distribute for the purpose of trade or any other purpose that will affect prejudicially the interests of the copyright holder/broadcaster
- exhibit such a circumvention device in public by way of trade
- import a circumvention device.

The Australian regulations also prohibit the offering of circumventing services, and the making available online of a broadcast device to an extent that will prejudicially affect the subscription broadcaster.

In addition, an activity is not considered an offence unless it was performed intentionally ("… 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 subscription broadcaster").

No distinction is made between unauthorised activities for commercial purposes and those for private purposes.

CA services and the interests of third parties
Australia has adopted several provisions in order to maintain the balance between protecting the interests of third parties and the use of CA devices, particularly where the public interest (law enforcement, national security) and the exercise of general exceptions as provided under copyright law are concerned. The provisions also allow for certain exceptions.

Under the Australian law, the prohibitions on the production and marketing of decoding devices do not apply where purposes of law enforcement or the public interest are at stake (Article 135 AN Subsection 2: "This Article does not apply in relation to anything lawfully done for the purpose of law enforcement or national security by or on behalf of: a) the Commonwealth or a State or territory; or b) an authority of the Commonwealth or of a State or Territory").

Additionally, in the case of the protection of CA devices used for copyright reasons, the manufacture, distribution, etc. of decoding devices is not unlawful under the condition that:

a) the person supplying decoding devices or services has signed a declaration stating that the device or service is to be used only for a permitted purpose while indicating at the same time what purpose this is, or
b) if the construction or import of a circumvention device is performed for only a permitted purpose or for the purpose of enabling a person to supply the device or to supply a circumventing device for use only for a permitted purpose (Article 116A 3 and 4).

In this context, it is a 'permitted purpose' if the device or service is used for the purpose of performing an act comprised in the copyright in a work or other subject matter and that such performance is in accordance with the copyright.

Sanctions/Remedies

Sanctions
If an infringing activity under Article 135 AS (CA used by providers of pay services) is carried out, monetary fines of not more than 550 penalty units and/or imprisonment for not longer than 5 years can be imposed, whereas no criminal sanctions are foreseen in the case of circumventing CA devices used to protect copyrights (Article 116D).

Civil remedies
For both variants of infringing activities, the Act provides for civil remedies, such as injunction, damages as well as compensation for loss of profit or additional damages.

Procedural provisions
In the case of CA techniques applied for copyright reasons, an action can be brought not only by the rightholder but also by the licensee of the copyright. This is of particular importance in cases where e.g. a service provider tries to combat circumventing activities against the broadcast service, but has no own intellectual property rights in the content of the service.

Secondly, the Australian law takes into account the sometimes difficult situation regarding burden of proof in cases of infringing activities. According to Article 135AS Subsection 3, "the only burden of proof that a defendant bears … is the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter in question exists."

Case law
No case law has been reported on acts of circumvention of free CA services provided on the basis of CA techniques.

2.2.2.

Canada

Introduction

In Canada, specific legislation on the legal protection of CA devices is embodied in two laws, i.e. the Radiocommunications Act (1.) and the Penal Code (2.). Whereas unauthorised decoding and certain preparatory activities are subject to the Radiocommunications Act, unauthorised reception is covered by Article 326 Criminal Code.

1. Radiocommunications Act

Details

Title: Article 9 Radiocommunications Act L.R.C., c. R-2
Date: 1985
Source: http://canada.justice.gc.ca/FTP/EN/Laws/Chap/R/R-2.txt
Classification: Telecommunications law

Scope of protection

Services protected
Encrypted subscription television or radio broadcasting signals are protected, but IS services are not. In this context, 'encrypted' is broadly defined as "treated electronically or otherwise for the purpose of preventing intelligible reception". Thus, the definition does not focus on specific techniques, such as encryption techniques.

Protection of free CA services
Protected are only such services which can be received upon payment of a subscription fee or other charge.[98] The notion of "or … against … other charge" could be interpreted in a way to also cover services which do not require a direct remuneration, such as public broadcasting services (payment of an indirect licence fee).

Reasons protected
Protection is not conditional on the reason it serves. The Radiocommunications Act does not focus expressly on the specific reason why the technology is protected (such as to ensure remuneration interests).

The general interests which underlie the Radiocommunications Act are—apart from ensuring remuneration interests—the protection of data and communication, intellectual property rights, and the protection of the economic interests of service providers, such as targeting markets, collecting information, controlling access to content, etc.

[98] Article 2 – Definitions: "subscription programming signal means radiocommunication that is intended for reception either directly or indirectly by the public in Canada or elsewhere on payment of a subscription fee or other charge".

Definitions
'Encrypted' means "treated electronically or otherwise for the purpose of preventing intelligible reception".

'Subscription programming signal' means "Radiocommunication that is intended for reception either directly or indirectly by the public in Canada or elsewhere on payment of a subscription fee or other charge" (Article 2 Radiocommunications Act).

Unlawful activities
Under Article 9 Radiocommunications Act, it is illegal to:
- decode a protected signal without authorisation from the service provider (Article 9 Section 1c)
- operate a radio apparatus so as to receive signals which have been decoded without authorisation (Article 9 Section 1d)
- retransmit to the public signals which have been decoded without authorisation (Article 9 Section 9c)
- without lawful excuse, manufacture, import, distribute, lease, offer for sale, sell, install, operate or possess any equipment or device which has been used or is intended to be used to decode programming signals without authorisation (Article 10 Section 1b).

Article 9 does not distinguish between infringements made for private purposes and those made for commercial purposes.

CA services and the interests of third parties
The Radiocommunication Law foresees certain exceptions from the prohibition to decode with regard to the availability of information. Under Article 10 Section 2.3, it is stated that "No person who decodes an encrypted subscription programming signal in contravention of paragraph 9(1)(c) shall be convicted of an offence under that paragraph if the lawful distributor had the lawful right to make the signal available, on payment of a subscription fee or other charge, to persons in the area where the signal was decoded but had not made the signal readily available to those persons." In other words, in a situation where persons in this area could not access a program even if they were willing to pay the fee because the broadcaster fails to make a programme available, those persons are apparently entitled to decode the signal themselves.

This exception does not apply to the ban on preparatory activities, such as the manufacture, import, distribution, lease, offer for sale or sale of any decoding equipment or device or component thereof (Article 10 Section 2.4).

Sanctions/Remedies

Sanctions
Offences against the mentioned provisions are considered an offence and can be punished upon summary conviction. Sanctions vary depending on whether the offence was committed by an individual or a corporation (higher sanctions for the latter). Furthermore, in case of continuous offences, a separate fine will be imposed for each day on which the offence is committed or continued.

An individual who unlawfully manufactures, imports, leases, offers for sale, sells, installs, modifies, operates or possesses a decoding device that has been used or is intended for use in

order to decode without authorisation, is liable to a fine not exceeding § 5000 or imprisonment for a term not exceeding 1 year, or to both; if a corporation commits such an offence, the fine can be as much as $ 25.000.

An individual who decodes encrypted signals without authorisation or operates a radio apparatus in order to receive such decoded signals is liable to a fine not exceeding $ 10.000 or to imprisonment for a term not exceeding 6 months, or to both; if a corporation commits such an offence, the fine can be as much as $ 25.000.

An individual who retransmits to the public unlawfully decoded programming signals is liable to a fine not exceeding C$ 20.000 or to imprisonment for a term not exceeding 1 year, or to both; if a corporation commits such an offence, the fine can be as much as $ 200.000 (Article 10 Sections 1, 2, 3).

Civil remedies
In addition, a person who has suffered loss or damage as a result of the offence may sue in any court with competent jurisdiction for damages from the person who engaged in the infringing conduct; the court may grant an injunction or order the infringer to pay compensation, or impose any other remedy it considers appropriate. In this context, the Federal Court is the court with competent jurisdiction. A monetary judgement may not exceed one thousand dollars if the person is an individual and did not commit the offence for commercial gain (Article 18 Section 1).

Procedural provisions
Under Article 18 Section 1, an action can be brought by any person who:
- holds an interest in the content of a subscription programming signal by virtue of copyright
- is authorised by the lawful distributor of a subscription programming signal to communicate the signal to the public
- holds a broadcasting license, or
- develops, manufactures, supplies or sells encoding or decoding devices.

The record of proceedings of any court in which the person against whom the action is brought was convicted is, in the absence of any evidence to the contrary, proof that that person was engaged in the infringing activity (Article 18 Section 3).

In Section (2.5) of Article 10, it is furthermore stated that no person shall be convicted of an offence if that person exercised all due diligence to prevent the commission of the offence. As a result, this means a reversal of the onus of proof. Potential infringers have to/or are entitled to prove that an offence was not committed intentionally.

Case law
No case law relevant to the provisions discussed above has been reported.

2. Articles 326, 327 Criminal Code

Details

Title: Articles 326, 327 Criminal Code

Date: Updated August 1999
Source: http://canada.justice.gc.ca/FTP/EN/Laws/Chap/C/C-46.txt
Classification: Penal law
Remarks: The provision does not focus specifically on services provided on the basis of CA but on signal theft. Article 326 is dealing with signal theft, whereas Article 327 bans certain preparatory activities facilitating signal theft

Scope of protection

Services protected
Articles 326 and 327 protect 'telecommunication'. In this context, telecommunication services are defined broadly as "any transmission, emission or reception of signs, writing images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system". Consequently, broadcasting services are included. The same may apply to IS services.

Protection of free CA services
Under the Canadian Penal Code, free CA services are protected against signal theft, but not against preparatory activities. This is since illicit devices as addressed by Article 327 must have been intended to "be used to obtain the use of any telecommunication facility or service without payment of a lawful charge therefor". Whereas Article 326 addresses generally the unlawful obtaining of any telecommunications service irrespective of whether this service is provided against payment or not.

Reasons protected
Article 326 (signal theft) is not specifically directed at the protection of any particular reason, whereas Article 327 (preparatory activities, such as the manufacture and distribution of illicit devices) exclusively protects remuneration interests.

Unlawful activities
Article 326 Criminal Code considers as theft the unauthorised use of protected services. In this context, no distinction is made between unauthorised activities for commercial purposes and those for private purposes.

According to Article 327 Criminal Code, any person who manufactures, sells, possesses or offers for sale devices designed to receive without authorisation and without the payment of a fee, is guilty of an indictable offence.

Sanctions/Remedies

Sanctions
Offenders are liable to imprisonment for a term not exceeding 2 years. In addition, the law provides for the forfeiture of the infringing devices.

Case Law
No case law has been reported on acts of circumvention of free CA services provided on the basis of CA techniques.

Future legislation

At the moment, there are no plans to adopt additional legislation on the legal protection of CA services.

2.2.3.

Japan

Introduction

Japan has recently adopted a specific provision on the legal protection of CA devices. This new provision—which is part of the Japanese competition law—does not distinguish between signals which are provided against payment and those which are not. Thus, the law also protects the providers of free CA services which use CA devices for non-remuneration interests.

Details

Title: Unfair Competition Act 1998
Date: 1998
Classification: Competition law

Scope of protection

Services protected
Covered are television and radio broadcasting services, but not IS services.

Protection of free CA services
Protection is granted whether or not services are provided against payment.

Reasons protected
Protection is not conditional on which reason the technology serves. The general interest behind the law is to protect the economic interests of service providers, such as the targeting of markets, collecting information, controlling access to content, ensuring exclusivity, etc.

Unlawful activities
Under the Japanese law, the import, distribution, sale and rental of decoding devices is prohibited. In this, the law focuses on activities linked to the process of making decoding devices available. However, neither the manufacture nor the use/possession for private/commercial purposes is covered.

The legislation focuses on commercial activities; private acts of circumvention are not covered.

CA services and the interests of third parties
The Japanese law includes a provision intended to stimulate/not hinder science and technological development. According to Article 11 (1) 7, under certain conditions the distribution or sale of decoding devices is lawful provided said devices are used for experimental purposes.

In addition, protection is restricted to devices which are *exclusively* used for the purpose of unauthorised circumvention (Article 2 (1) (10) (11).

Sanctions

Sanctions
Monetary fines can be imposed.

Civil remedies
In addition, it is possible to apply for injunction.

Case law
No case law applying to these provisions is known.

Future legislation

At the moment, there are no plans to adopt additional legislation on this issue.

2.1.4.

United States of America

Introduction

In the US, legal protection of encrypted broadcasting services is contained in two provisions of the Telecommunications Act 1934 (TCA), as amended by the Telecommunications Act 1996. The original purpose of these provisions was to protect the confidentiality of communication against unauthorised interception. The Federal Communications Commission (FCC) then decided that also television services, particularly pay-TV services, would fall under the TCA (Federal Communications Commission Public Notice, 43 Fed. Reg. 46, 581 (1978)). This decision has been upheld by several courts.

Whereas the underlying idea is to protect, apart from confidentiality reasons, also the use of CA devices for remuneration reasons, the wording of the law does not make protection conditional on the existence of a remuneration interest. Consequently, also free CA services which use CA devices may be protected.

Further provisions on the legal protection of the use of CA devices are implemented in Section 1201 (a) Digital Millennium Copyright Act 1998 (DMCA). This provision was adopted in the framework of the implementation of Article 11 WCT and Article 18 WPPT. Similar to the WCT and WPPT, however, Article 1201 (a) does not deal with the protection of the rights of broadcasting organisations and other service providers, but only those of rightholders, performers and phonogram producers. The DMCA includes a number of exceptions which are particularly focused on the use of CA devices and certain third parties interests.

1. Article 633 Telecommunications Act 1934

Details

Title: Telecommunications Act 1934, as amended by Telecommunications Act 1996
Date: 1996
Source: Pub. LA. No. 104-104, 110 Stat. 56 (1996), see also: http://www.fcc.gov/telecom.html
Classification: Telecommunications law

Scope of protection

Services protected
Article 633 Telecommunications Act 1934 protects any communications services offered over a cable system, including television broadcasting services. In addition, the provision is sufficiently broad to probably also cover IS services. It is not explicitly required that protected services are based on any form of access control. However, also access controlled services fall under the provision.

Protection of free CA services
Protection is not conditional on the existence of a remuneration interest. Consequently, also free CA services may claim protection.

Reasons protected
Originally, the underlying reasoning for the provision was to protect the confidentiality of communication; later, also remuneration interests were considered subject to protection.

Nevertheless, according to the wording of Section 633, protection is not conditional on the existence of a remuneration or other particular interests. Thus, Article 633 may be applied in situations where CA devices serve other reasons, such as the protection of minors (see below).

Definitions
"Assist in intercepting or receiving" shall include the manufacture or distribution of equipment intended by the manufacturer or distributor (as the case may be) for unauthorised reception of any communications service offered over a cable system in violation of subparagraph (1) (Section 633 (a) (2))."

Unlawful activities
Prohibited are the unauthorised act of interception or reception of a protected service as well as assisting in such acts. 'Assisting' includes the "manufacture or distribution of equipment intended by the manufacturer or distributor for unauthorised reception of a protected service" (Section 633 (a) (1)).

CA services and the interests of third parties
Article 633 includes an open clause concerning the protection of general public interests (""unless … as may otherwise be specifically authorised by law").

Sanctions/Remedies

Sanctions
Any person who wilfully commits an offence can be fined a maximum of $ 1,000 or be sentenced to imprisonment for not more than 6 months, or both. If the offence was committed for commercial purposes, the fine can be increased to $ 50,000 and the length of imprisonment to 2 years, or both (Section 633 (b) (1, 2)).

Civil remedies
Any person aggrieved by a violation may bring a civil action in a US district court or in any other court of competent jurisdiction. The court may grant injunctions and award damages (in case of statutory damages, between $ 250 and $ 10.000' in case of commercial activities, not more than $50.000). Penalties can be reduced if the court finds that an infringer was not aware and had no reasons to believe that he/she was committing a violation.

Case law
No case law has been reported on the application of this rule on acts of circumvention of a free access controlled service.

2. Section 705 Telecommunications Act 1934

Details

Title: Telecommunications Act 1934, as amended by Telecommunications Act 1996
Date: 1996
Source: Pub. LA. No. 104-104, 110 Stat. 56 (1996)
Classification: Telecommunications law

Scope of protection

Services protected
Protected are any interstate or foreign communication by wire or satellite, including television services. It is not explicitly required that programmes are encrypted, though it can be concluded from the context that encrypted services are included.

Protection of free CA services
Protection is not conditional on the existence of a remuneration interest. Thus, also free CA services which use encryption may fall under this provision.

Reasons protected
Originally, the underlying reasoning for the provision was the confidentiality of communication; later, also remuneration interests were considered subject to protection.

The provision, as mentioned, does not explicitly link protection to the existence of a particular interest. Thus, Article 633 may be applied also where CA devices serve other reasons.

Definitions
'Encrypt' means to "transmit such programming in a form whereby the aural and visual characteristics (or both) are modified or altered for the purpose of preventing the unauthorised reception of such programming by persons without authorised equipment which is designed to eliminate the effects of such modification or alteration".

Unlawful activities
It is prohibited to intercept, receive, assist in receiving (see definition above), transmit or assist in transmitting protected services, as well as to use such communication for own benefit or the benefit of another not entitled thereto. In addition, it is unlawful to publish the existence, contents, substance, purport, effect or meaning of such services (Section 705 (1)).

Furthermore, it is unlawful to manufacture, assemble, modify, import, export, sell or distribute any electronic, mechanical or any other device or equipment with the knowledge, or with reason to know, that the device or equipment is primarily of assistance in the unauthorised decryption of satellite cable programming or direct-to-home satellite services (Section 705 (4)).

CA services and the interests of third parties
Section 705 (c) deals with the encryption of public broadcasting and the accessibility of such broadcast to the public. No person shall encrypt or continue to encrypt satellite-delivered programmes included in the National Program Service or the Public Broadcasting Service and

intended for public viewing by retransmission by television broadcast stations; unless at least one unencrypted satellite transmission of any programme subject to this subsection is provided; this subsection shall not prohibit additional encrypted satellite transmissions of the same programme.

In other words, it has to be ensured that public service television programmes are accessible to the public in unencrypted form. However, it is allowed to *additionally* transmit the same programme in encrypted form, e.g. in the framework of a digital programme bouquet.

Sanctions/Remedies

Sanctions
Infringers can be fined up to $ 2.000 or imprisoned for not more than 6 years ($ 50.000 / 2 years if carried out for commercial purposes). In case of activities in the context of the unauthorised decoder business, higher penalties can be imposed (i.e. up to $ 500.000 / 5 years of imprisonment).

Civil remedies
Any person aggrieved by any violation may bring a civil action in a US district court or in any other court of competent jurisdiction. The court may grant injunctions and award damages. Damages can include actual damages suffered as a result of the violation as well as any profits. In case of statutory damages, fines can range from $ 1,000 to $ 10,000 (and up to $ 100,000 if the infringement was carried out for commercial purposes). Where courts find that the violator was not aware and had no reason to believe that his/her act constitutes a violation, damages may be reduced to no less than $ 250.

Remarks
The Telecommunications Act also includes obligations to scramble certain programmes or channels. For example, upon request by a cable service subscriber, a cable operator shall, without charge, fully scramble or otherwise block the programming of each channel in order to prevent persons other than subscribers from receiving it (section 640 (a)).

Another provision applies in respect to the protection of minors. Providers of sexually explicit adult programming shall fully scramble or otherwise block the programme so that only subscribers can receive it (Section 641 (a)).

3. Section 1201 (a) Digital Millennium Copyright Act

Details

Title: Digital Millennium Copyright Act (DCMA)
Date: 1998
Source: Publ. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998)
Classification: Copyright law
Remarks: The provisions on the protection of technological measures are included in the WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998, which is part of the DCMA. However, the DCMA does not deal with technological measures as used by broadcasters, since the rights of broadcasters are not subject to either the WCT or

the WPPT. The provisions on acts of unauthorised circumvention under Section 1201 (a) DCMA will become effective on 28 October 2000.

Scope of protection

Services protected
Section 1201 DCMA does not address particular services which use technological measures, but focuses on a situation in which technological measures are used by rightholders to protect a work that is subject to copyright protection.

Section 1201 divides technological means into two categories: measures that prevent unauthorised use of a protected work (Section 1201 (b)) and those that prevent unauthorised access to works. The latter measures are dealt with in Section 1201 (a) DCMA and will be described in the following.

Rightholders in the sense of Section 1201 are rightholders, performers and producers of phonograms, not e.g. broadcasting organisations. This is because the provisions implement the WCT and WPPT, while the DCMA does not deal with adequate rights of broadcasting organisations.

Reasons protected
The DCMA focuses on the protection of technological measures used for reasons of copyright protection.

Definitions
'Circumvention of a technological measure' means to "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measures, without the authority of the copyright owner".

A technological measure "effectively controls access to a work" if the measure in the ordinary course of its operation requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

Unlawful activities
Prohibited are both the act of circumvention of CA devices as well as certain preparatory activities. It is illegal to manufacture, import, offer to the public, provide or otherwise traffic illicit devices which are:
- primarily designed or produced for the purpose of circumventing,
- have only limited commercially significance or a use other than to circumvent,
- are marketed for use in circumventing.

The act of circumvention shall not be unlawful if users of protected works are adversely affected in their ability to make non-infringing uses of that work.

CA services and the interests of third parties
The prohibitions contained in Section 1201 (a) are subject to a number of exceptions which deal specifically with the implementation of CA devices. The broadest of these exceptions, as contained in Section 1201 (a) (1) (B) (E), establishes an ongoing administrative rule-making procedure to evaluate the impact of the prohibition against the act of circumventing such access control measures.

Six additional exceptions are as follows:

1. Non-profit libraries, archives and educational institutions (Section 1201 (d)). The prohibition on the act of circumvention of access control measures is subject to an exception that permits non-profit libraries, archives and educational institutions to circumvent solely for the purpose of making a good-faith determination as to whether they wish to obtain authorised access to the work.
2. Reverse engineering (Section 1201 (f)). This exception permits circumvention and the development of technological means for such circumvention by a person who has lawfully obtained a right to use a copy of a computer program for the sole purpose of identifying and analysing elements of the program necessary to achieve interoperability with other programs, to the extent that such acts are permitted under copyright law.
3. Encryption research (Section 1201 (g)). An exception for encryption research permits circumvention of access control measures and the development of the technological means to do so, in order to identify the flaws in and vulnerabilities of encryption technologies.
4. Protection of minors (Section 1201 (h)). This exception allows a court when applying the prohibition to a component or part to consider the necessity for its incorporation in technology that prevents access of minors to material on the Internet.
5. Personal privacy (Section 1201 (i)). This exception permits circumvention if the technological measure or the work it protects is capable of collecting or disseminating [personally identifying information about the online activities of a natural person. = information which identifies a natural person who is carrying out online activities.?]
6. Security testing (Section 1201 (j)). this exception permits circumvention of access control measures and the development of technological means for such circumvention for the purpose of testing the security of a computer, computer system or computer network, with the authorisation of its owner or operator.

Sanctions/Remedies

Sanctions

It is a criminal offence to violate Sections 1201 and 1202 wilfully and for purposes of commercial advantage or private financial gain. Under Section 1204, penalties include a fine of up to $ 500.000 or up to 5 years of imprisonment for a first offence, and a fine of up to $ 1.000.000 or up to 10 years of imprisonment for subsequent offences. Interestingly, non-profit libraries, archives and educational institutions are entirely exempt from criminal liability (Section 1204 (b)).

Civil remedies

Any person injured by a violation of Section 1201 may bring a civil action in a federal court. Section 1203 gives courts the power to grant a range of equitable and monetary remedies similar to those available under the Copyright Act, including statutory damages. The court may reduce damages in cases of innocent violations, where the violator proves that he/she was not aware and had no reason to believe that his/her acts constituted a violation. Special protection is given to non-profit libraries, archives and educational institutions, which are entitled to a complete remission of damages in these circumstances (Section 1203 (c)).

Case law

Because Article 1201 is relatively new, not much case law exists on this provision. The only case reported does not deal with broadcasting or IS services but with access control applied to DVDs, and therefore has no relevance to the purpose of this study.

Annex II

Introduction to the questionnaires

This questionnaire is part of a study performed by IViR on the use of conditional access systems for non-remuneration reasons. The aim of the study is to examine the legal and economic implications of such use within the Internal Market and the need to introduce specific legal protection.

Both the study and the questionnaire were commissioned by the European Commission, G D XV.

In recent years, providers of broadcasting and information society services have increasingly relied on the use of conditional access devices when providing services. Conditional access devices enable their users to control who may access an electronically transmitted content or service, and under which conditions. There are various reasons to control access to contents or service, ranging from ensuring remuneration, targeting markets, identifying consumers, enhancing the security of services and infrastructure, complying with legal and contractual obligations, etc. Not surprisingly, conditional access devices are considered an efficient tool of rapidly growing importance to providers of services in the field of electronic commerce.

Conditional access systems, however, are increasingly exposed to piracy. As indicated in the Commission's Green Paper on encrypted services, a flourishing piracy industry manufactures and markets various forms of decoding devices enabling unauthorised access to services and contents. To improve the legal protection of conditional access devices, the European Commission drafted the Conditional Access Directive, which was recently adopted. The directive introduces a common standard of protection against piracy for providers of conditional access based services and for providers of conditional access devices. The regulation, however, focuses exclusively on the protection of conditional access in a situation where access control is applied to serve the remuneration interests of service providers; it does not provide for the legal protection of access control mechanisms where they serve other interests.

As a result, the use of conditional access devices for non-remuneration reasons is subject to considerable legal uncertainty. Only a few member states have specific national legislation against the unauthorised circumvention of conditional access devices. As a result, particularly internationally operating providers of access controlled services as well as producers of conditional access devices may be confronted with various forms of piracy and yet have no adequate legal protection. Disparities regarding the level of protection in the member states of the EU may create serious obstacles to the development and free circulation of conditional access services or devices, as well as to competition within the Internal Market. On the other hand, where specific legislation in certain member states does exist, such legislation could impose restrictions on the provision of services from other member states.

In response, the European Commission commissioned this study in order to enable an objective assessment to be made as to whether or not there is a need to provide for additional and harmonised protection for conditional access.

Objective of the questionnaire

The objective of the questionnaire is to obtain information on conditional access devices used for non-remuneration reasons. This information is needed in order to examine the impact of conditional access devices on the Internal Market and its players, as well as the need to introduce additional legal protection at a European level.

The completed questionnaires will enable IViR:

- to evaluate possible market developments of conditional access devices and the increase in the number and types of services that can use conditional access;
- to evaluate the impact of these developments on the functioning of the Internal Market (impact on competition, on consumer choice and access to contents/services provided from other member states);
- to assess the extent to which conditional access devices used for non-remuneration reasons are threatened by piracy;
- to analysis the existing legal protection of conditional access devices as well as the impact of such legislation on the Internal Market;
- to assess whether and, if so, to what extent there is a need to introduce additional legal protection for service providers using conditional access and for providers of conditional access as a service in its own right.

On the basis of this analysis, IViR will develop its conclusions and submit recommendations to the European Commission.

Means of reply

Your comments on this questionnaire will be highly valued. We would ask you to take the time to read the questions carefully and to be as precise as possible in your answers.

Please tick the relevant responses or give a short answer and provide any additional information and comments you wish to make at the end of each part. Please make the answers reasonable succinct whilst covering the relevant points.

Please indicate at point two if you wish us to keep your response confidential in particular as regards a possible publication of the results of the study. Confidentiality also implies that your answers will not be made available to the European Commission.

The text of the questionnaire can be obtained in electronic form by sending us a request at the following e-mail address: helberger@jur.uva.nl.

Please address your response to us before **…** at the e-mail address above or forward by fax to IViR on 0031 20 5253033 or post to the following postal address:
Institute for Information Law - IViR
Ms. Natali Helberger
Rokin 84
1012 KX Amsterdam
The Netherlands

If you have any further questions, please do not hesitate to contact us at the e-mail address above or by telephone under 0031 20 5253643 (Ms Natali Helberger).

Thank you very much for your assistance.

1 **Name of organisation:** ……
……...……
Name and function of contact person: …..……
……..……
E-mail address: ……..……..
Tel. and fax nos: ……...…….
Country: ……..……

2 **Do you wish us to keep your reply confidential?**
- ❑ Yes
- ❑ No

DESCRIPTION OF YOUR MAIN FIELD OF ACTIVITY

3 **Please indicate your main field of activity:**
- ❑ Television broadcasting Pay/Free
- ❑ Radio broadcasting Pay/Free
- ❑ Information society service:[99] (Please briefly explain what sort of service) ..…….. Pay/Free
……..
……..
……..
- ❑ Other/s: ..…….
- ❑ …….……

4 What is the territorial scope of your activity?
- ❑ Local: (Please briefly explain) ……
- ❑ National: (Country) ..……...
- ❑ Transnational:
  - ❑ European Union Countries:
  - ❑ Austria
  - ❑ Belgium
  - ❑ Denmark
  - ❑ Finland
  - ❑ France
  - ❑ Germany
  - ❑ Greece
  - ❑ Ireland
  - ❑ Italy
  - ❑ Luxembourg
  - ❑ Netherlands
  - ❑ Portugal

[99] Information Society Service is defined as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

- ❑ Spain
- ❑ Sweden
- ❑ United Kingdom

- ❑ Other European Countries: …….
- ❑ …….
- ❑ …….
- ❑ Other Countries: ……..

IMPLEMENTATION OF CONDITONAL ACCESS DEVICES

5 **Do you use one or more conditional access devices[100] in your activity?**
Which ones ? (Please briefly explain the supplier/s and the device/s used)
……...
……...
……...
……...
……...
……...
……...

If not, then go directly to question 16.

6 **What type of device/s?**
- ❑ Password device
- ❑ Encryption device
- ❑ Evaluation and filtering device
- ❑ Device based on biometrics
- ❑ Other device, namely ……...

…….
…….

7 **For what types of activity do you use the mechanism/s?**
- ❑ For broadcasting or information society services that you implement.
- ❑ For the exchange of information internally.

At what level in the company (administration, R&D, Sales and Marketing, …)?
……..
……..…….

8 **For what reason/s?** (Several answers possible)
- ❑ To ensure payment of services
- ❑ Targeted distribution of services
- ❑ Identification of users
- ❑ Collecting information
- ❑ Data protection
- ❑ Property protection, e.g. intellectual property rights
- ❑ Security of communication
- ❑ Protection of firm-owned soft-/hardware (internal infrastructure)

[100] Conditional access device means any equipment or software designed to give access to a protected service in an inteligible form.

- Security of commercial transactions
- To comply with legal/contractual obligations
- Other/s: (Please briefly explain)…….
- …….
- ……..……...

9 **If you use conditional access devices for more than one reason: Do you apply the same conditional access device/s to serve several reasons at the same time?**

- The same conditional access device serves different reason at the same time.
- We have implemented different conditional access devices to serve different reasons.

10 **Would you consider to implement conditional access devices exclusively to serve non-remuneration reasons?**

- Yes (Please explain for which reason, see e.g. list in question 8)……..
  ..……..
- No (Please state your reason) ……..……
  ……..……..
  ……...
  ……..……..
  ……...
  ……...

ECONOMIC IMPACT OF CONDITIONAL ACCESS

11 **What economic advantages do you expect from the implementation of conditional access devices for non-remuneration reasons?**……
……..……..……
……..……..
……...……
……...
……...

12 **What is the estimated economic value of the goods/services so protected (in Euro)?** (Please mention what are you basing the calculation of this estimation on).
……..…….....
……..…….....
.....….....
……...
……...

13 **In your opinion, can a conditional access device also be used:**

To modify the competition in your favour?	Yes/No
To create an entry barrier insurmountable for new entrants?	Yes/No
To better control consumers' choices and limit the possibilities of use?	Yes/No
To reinforce market power / level of market domination?	Yes/No
To better know and control the behaviour of each consumer/user of the service?	Yes/No
To enable more differentiated services?	Yes/No
To enable a more differentiated pricing policy?	Yes/No

Other/s:…….

……
……..

If yes, in what way and in which market configuration? Give an example, please.
……...
……...
……...
……...
If no, why? ……..……..
……...
……...
.....

14 **What will be the effect of an increased use of conditional access by other market players on your organisation?**
……...
……...
……...
……..
……..
……...

15 Do you intend, in the short to medium term, to change the conditional access device/s of the service that you operate?
- ❑ Yes
- ❑ No

16 **If you have not implemented conditional access devices yet, do you intend to do so?**
- ❑ In the short term
- ❑ In the medium term
- ❑ In the long term

For what reason/s (see e.g. list in question 8)?……..……..
……...
……..……..

THE PROBLEM OF ILLICIT ACCESS TO CONDITIONAL ACCESS SERVICES

17 **Do you know of any cases of piracy as regards conditional access devices you have implemented?**
- ❑ No
- ❑ Yes
- ❑ If yes:

What was/were the exact reason/s, for which the particular device has been implemented (see e.g. list in question 8)?…….…….
……...

18 **Please briefly explain the forms of piracy.** (Please indicate what is correct)

- ❑ Manufacture/ import/ distribution/ sale/ rental/ possession for commercial purposes of illicit devices[101]
- ❑ Installation/ maintenance/ replacement for commercial purposes of an illicit device
- ❑ Use of commercial communication to promote illicit devices
- ❑ Use/possession of illicit devices for commercial purposes
- ❑ Use/possession of illicit devices for private purposes
- ❑ Other/s: ……...

.....……..…
……..……..……
……..……..

19 How would you describe the consequences of piracy for your activity? (Several answers possible)

- ❑ Loss of subscription fees/advertisement fees/income
- ❑ Loss of credibility/confidentiality
- ❑ Loss of clients
- ❑ Legal consequences because of breach of contractual/statutory obligations (e.g. legal actions)
- ❑ Need/time/costs to replace pirated device
- ❑ Financial harm for third parties involved, e.g. rightholders (Please briefly explain)……..……
  ……...….
- ❑ Other/s:..……..……
- ❑ …….
……..

20 **Can you specify the general amount of damages suffered (in Euro)?**…….....
……...

SOLUTIONS PROVIDED BY NATIONAL LAW

21 Does specific legislation on the protection of conditional access devices exist in your country?

- ❑ Exist
- ❑ Do not exist
- ❑ Do not know

<u>If no specific protection exists, then go directly to question 23.</u>

22 **Do you consider the existing legal protection of conditional access devices effective in the fight against piracy?**

- ❑ No
- ❑ Yes

Please state your reason: ……..
……..
……..
……...
……...

[101] Illicit device shall mean any equipment or software designed or adapted to give access to a protected service in an intelligible form without authorisation of the service provider.

……...
……...
……...
……..
……..

THE OPERATION OF THE INTERNAL MARKET: OBSTACLES TO THE FREE MOVEMENT OF CONDITIONAL ACCESS SERVICES

23 If you are providing transnational services: Have you experienced any problems over the last few years due to absence/disparity of legal protection of conditional access in other countries? (Several answers possible)

- ❑ No
- ❑ Yes: Country .....
- ❑ If so, what was the impact felt:
  - ❑ Increased threat of piracy in these countries
  - ❑ Increased need of legal research into national laws
  - ❑ Negative impact on negotiating position, e.g. when acquiring program rights for these countries
  - ❑ Import of illicit devices[102] from member states where no/lower standard of legal protection exists
  - ❑ Distortions of competition between service/content providers in different countries
  - ❑ Need to refrain from activities in <u>specific</u> countries. Country/ies:.....
  - ❑ Others (Please briefly explain)…….…….
  - ❑ ……..……..
  - ❑ ……..……..

  …….……

24 **Have you experienced any difficulties to obtain/enforce legal protection in another country?** (Please briefly explain)

…….....
.....
……...
……...
……..
……...

25 **What is the consequence of absence/disparity of legal protection in other states for the marketing and security policy of your organisation?** (Several answers possible)

- ❑ No impact
- ❑ Refraining from covering territories providing for a lower standard of protection
- ❑ Seeking to increase the efficiency of own conditional access devices
- ❑ Applying other techniques beside/instead of conditional access devices: (Please briefly explain) ……..

  ……..
- ❑ Contractual solutions ……..

[102] Illicit devices means any equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorisation of the service provider.

- Others: …….
- ……
…..…….

26 **Are you of the opinion that additional legal protection for conditional access devices serving non-remuneration interests is needed?**

- No
- Yes

27 **What sanctions/remedies are needed?**

- Monetary fines
- Prison sentences
- Administrative provisions
- Civil provisions: (Please briefly specify)……
  ……
  ……

Space for further remarks: ……
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...

Please send your reply to:

Institute for Information Law (IViR)
Ms Natali Helberger
Rokin 84
NL-1012 KX Amsterdam
or:
fax: + 31 20 525 3033
or:
e-mail: helberger@jur.uva.nl

Annex III

Questionnaire to National Correspondents

1 **Name of organisation**:…….
……..…….
Name and function of contact person: …..…..……..
……..……..
E-mail address:……...…….
Tel. and fax nos: ……...…….
Country: ……...

2 **Do you want us to keep your reply confidential?**
- ❑ Yes
- ❑ No

DESCRIPTION OF YOUR MAIN FIELD OF ACTIVITY

3 **What is your field of activity?**
- ❑ Regulatory authority
  - ❑ Government
  - ❑ Other regulatory body
- ❑ University
- ❑ Scientific institute
  - ❑ Public
  - ❑ Private
- ❑ Legal adviser
  - ❑ In broadcasting organisation
  - ❑ Other/s:..……
    …….
    …….
- ❑ Law firm
- ❑ Other/s:..……..…….
……...
……..

DESCRIPTION OF EXISTING NATIONAL LAW

4 **Do regulations on the legal protection of conditional access devices exist in your country?**

- ❑ No
- ❑ Yes (Where applicable law exists, please attach a copy of the relevant rule.)

If no such legislation exists, please go to question **15**.

5 **What is the field of law in which specific legislation is introduced?**

- ❑ Penal law
- ❑ Civil law
- ❑ Administrative provisions
- ❑ Broadcasting law
- ❑ Telecommunication law
- ❑ Data protection law
- ❑ Other/s:…….……

6 **Which general reasons for using conditional access devices are subject to protection?** (Several answers possible)

- ❑ Remuneration interests
- ❑ Security of communication
- ❑ Data protection
- ❑ Secrecy and confidentiality of information
- ❑ Intellectual property rights
- ❑ Security of firm owned soft-/hardware, communication and information networks
- ❑ Security of financial transactions
- ❑ Economic interests of the service/content providers (e.g. targeting markets, collecting information, controlling access to contents, ensuring exclusivity, etc.)
- ❑ Other interests: (Please briefly explain which)……..…….
- ❑ …….
- ❑ …….
- ❑ No distinction is made between the reasons conditional access devices serve.

7 **Which signals are protected?** (Several answers possible)

- ❑ Television broadcasting signals
- ❑ Radio broadcasting signals
- ❑ Other/s:……..…….

8 **Are the signals only protected if they are provided against payment?**

- ❑ Yes
- ❑ No

9 **What activities are subject to legislation?** (Several answers possible)

- ❑ Unauthorised interception of protected signals
- ❑ Manufacture of decoding devices
- ❑ Import of decoding devices
- ❑ Distribution of decoding devices
- ❑ Sale of decoding devices
- ❑ Rental of decoding devices
- ❑ Possession of decoding devices
- ❑ Installation of decoding devices
- ❑ Maintenance of decoding devices
- ❑ Replacement of decoding devices
- ❑ Use of commercial communications to promote decoding devices
- ❑ Other/s:…...……..……...
- ❑ …….
- ❑ …….

10 **Does the existing legislation focuses exclusively on commercial activities to enable the unauthorised circumvention of conditional access devices (such as manufacture, sale etc. of decoding devices)?**

- ❑ Existing legislation addresses exclusively commercial activities.
- ❑ Existing legislation addresses exclusively the unauthorised circumvention by individuals, i.e. for private purposes.
- ❑ No distinction is made between unauthorised activities for commercial and private purposes.

11 **What is the nature of sanctions/remedies foreseen?** (Several answers possible)

- ❑ Monetary fines: ……...
- ❑ Prison sentences: …….
- ❑ Administrative provisions: ……..
- ❑ Civil provisions: ……..
- ❑ Other/s:...…….
- ❑ No sanctions are provided.

12 **Do the regulations take into account any third party interests which may be affected by the use of conditional access devices (e.g. by stating exceptions)?**

- ❑ No.
- ❑ Yes: (Please briefly explain).……..……..……..

……...
……...
……...
……...
……..……..

13 **Do you know of any case law applying these specific regulations?**

- ❑ No
- ❑ Yes: (please give a reference/s and/or a short description)……..……..
……..…
……..…
……..……..…
……..
……...…
……...
……...

14 **Do you consider existing legislation on the legal protection of conditional access devices appropriate and efficient?**

- ❑ Yes
- ❑ No

Please briefly explain, why you think that existing regulations are appropriate/not appropriate. ……
……...
……...
……...
……...
……...
……...
……...
……..
……..

15 **Where no specific legislation exists: What general rules are applied on cases of unauthorised circumvention of conditional access systems?**……...
……...
……...
……...
……...
……...

ENVISAGED (ADDITIONAL) LEGISLATION

16 **Is it envisaged that new/additional legislation on the legal protection of conditional access devices be introduced in the near future?**

- ❑ No
- ❑ Yes

If no such legislation is planned, please go to question 25.

17 **Which general reasons for using conditional access devices are subject to protection?** (Several answers possible)

- ❑ Remuneration interests
- ❑ Secrecy and confidentiality of communication
- ❑ Data protection
- ❑ Secrecy and confidentiality of information
- ❑ Intellectual property rights
- ❑ Security of firm-owned soft-/hardware, communications and information networks
- ❑ Security of financial transactions
- ❑ Economic interests of the service/content providers (e.g. targeting markets, collecting information, controlling access to contents, ensuring exclusivity, etc.)
- ❑ Other interests: (Please briefly explain which)……..…….
- ❑ …….
- ❑ …….
- ❑ …….
- ❑ No distinction is made between the reasons conditional access devices serve.

18 **Which signals are protected:** (Several answers possible)

- ❑ Television broadcasting signals
- ❑ Radio broadcasting signals
- ❑ Other/s:...…….……

19 **Are the signals protected only if they are provided against payment?**

- ❑ Yes
- ❑ No

20 **What activities are subject to legislation?** (Several answers possible)

- ❑ Unauthorised interception of protected signals
- ❑ Manufacture of decoding devices
- ❑ Import of decoding devices
- ❑ Distribution of decoding devices
- ❑ Sale of decoding devices
- ❑ Rental of decoding devices
- ❑ Possession of decoding devices
- ❑ Installation of decoding devices
- ❑ Maintenance of decoding devices
- ❑ Replacement of decoding devices
- ❑ Use of commercial communications to promote decoding devices
- ❑ Other/s:...……..……...
- ❑ …….

22 **Does the existing legislation focuses exclusively on commercial activities to enable the unauthorised circumvention of conditional access devices (such as manufacture, sale etc. of decoding devices)?**

- ❑ Existing legislation addresses exclusively commercial activities.
- ❑ Existing legislation addresses exclusively the unauthorised circumvention by individuals, i.e. for private purposes.
- ❑ No distinction is made between unauthorised activities for commercial and private purposes.

23 **What is the nature of sanctions/remedies?** (Please specify)

- ❑ Monetary fines: ……...
- ❑ Prison sentences: …….
- ❑ Administrative provisions: ……..
- ❑ Civil provisions: ……..
- ❑ Other/s:...…….

24 **Do the regulations take into account any third party interests which may be affected by the use of conditional access devices (e.g. by stating exceptions)?**

- ❑ No
- ❑ Yes: (Please briefly explain)……..……..

……...
……...
……...
……...
……...

Please provide references wherever possible.

NEED FOR FURTHER INITIATIVES

25 **Is there, in your opinion, a need to introduce additional legislation on the legal protection of conditional access devices?**

- ❑ Yes
- ❑ No

Please explain your reasons. …….
……...
……...
……...
……...
……...
……...

26 **Which general interest objectives do you consider legitimate grounds for protecting conditional access devices (see e.g. list in question 6)?** Please explain your reasons……...
…….
……..

27 **Do you see a need for further European Community activities as regards the legal protection of conditional access devices?**

- ❑ Yes
- ❑ No

Please explain your reason. ……...
……..……
……..……
……..……
……...
……...

28 **If you see the need for further action, should this be legislative measures (e.g. expanding the Conditional Access Directive) or others?**
……..……
……..……
……...
……..
……..

Space for further remarks: ……
……...
……...
……...
……...
……...
……...
……...
……...
……...
……..……
……...

Please send your reply to:
Institute for Information Law (IViR)
Ms Natali Helberger
Rokin 84
NL-1012 KX Amsterdam
or:
fax: + 31 20 525 3033
or:
e-mail: helberger@jur.uva.nl

Annex IV

Questionnaire to Consumer Organisations/Interest Groups

1 **Name of organisation:** .....…….....
……...
Name and function of contact person: .....……
……...
E-mail address: .....
Tel. and fax nos.: .....
Country: .....

2 **What is your field of activity?**

- ❑ Consumer protection
- ❑ Youth protection
- ❑ Broadcasting services
- ❑ Information society services
- ❑ Content providers
- ❑ Culture
- ❑ Competition
- ❑ Other/s: .....….....…
- ❑ .....…….....

3 **Do you wish us to keep your reply confidential?**

- ❑ Yes
- ❑ No

IMPACT OF CONDITIONAL ACCESS ON THE INTERNAL MARKET

4 **How do you assess the prospects of services based on electronic access control?**

……
……
…….
…….
…….
……..
……

5 **Do you believe that the increased use of conditional access by service providers will in any way affect the interests of the third parties involved**, **specifically:** (Please briefly explain your opinion)

❑ Relation/interests of competing service providers? YES/NO

.....
.....
.....
……...
……...

❑ Consumer choice? YES/NO

.....
.....
.....
……...
……

❑ Consumer access to services from other member states of the European Union? YES/NO

.....
.....
.....
……...
……

❑ Other/s?.....

.....
.....
.....
……...
……...

LEGAL PROTECTION OF CONDITIONAL ACCESS DEVICES

6 Are you aware of the existence of any specific legislation on the protection of conditional access devices against unauthorised circumvention:
In your country?

❑ Yes
❑ No

In other European Union countries?

❑ Yes
❑ No

If so, in which country/ies: ……..
.....…….....

7 **If such legislation exists, do you consider the applicable rules appropriate? In particular, do you think existing legislation provides sufficient protection to providers of conditional access services? Do you think the interests of the third parties involved (e.g. consumers, rightholders, competitors, etc.) are sufficiently taken into account? (**Please state your reasons).....…
.....
.....
.....
……...
……...
……...
……..
……...
……...
……...
……...
……...
……...

8 **Are you aware of any effect of such legislation on the interests of the parties concerned (users or producers of conditional access, consumers, rightholders, competitors, public entities)?** (Please briefly describe)
.....…….....
.....
.....
……...
……...
……...
……...
……...
……...
……...

9 **Is there current public or political debate in your country on the need to introduce new/additional legal protection for conditional access devices?**

- ❑ Yes
- ❑ No

10 **If so, what are the main objectives of such debate?** .....
.....
.....
.....
.....
.....…
……...
……...
……...
……...
……..

11 **Please state your point of view**.....……

.....
.....
.....
.....
.....
.....
.....
……...
……...
……...
……...
……...
……...
……...
……...
……...
...……
……...
……..

Please send your reply to:
Institute for Information Law (IViR)
Ms Natali Helberger
Rokin 84
NL-1012 KX Amsterdam
or:
fax: + 31 20 525 3033
or:
e-mail: helberger@jur.uva.nl

Annex V

1 **Name of organisation:** ……..
……...
Name and function of contact person: ……
……..…….
E-mail address: ……..…….
Tel. and fax nos: …..……..
Country*:* ……..

2 **Do you wish us to keep your reply confidential?**
- ❑ Yes
- ❑ No

DESCRIPTION OF YOUR FIELD OF ACTIVITY

3 What is the territorial scope of your activity?
- ❑ Local: (Please briefly explain)……
- ❑ National: (Country)..……...
- ❑ Transnational:
  - ❑ European Union Countries:
    - ❑ Austria
    - ❑ Belgium
    - ❑ Denmark
    - ❑ Finland
    - ❑ France
    - ❑ Germany
    - ❑ Greece
    - ❑ Ireland
    - ❑ Italy
    - ❑ Luxembourg
    - ❑ Netherlands
    - ❑ Portugal
    - ❑ Spain
    - ❑ Sweden
    - ❑ United Kingdom

  - ❑ Other European Countries:
  - ❑ ……...
  - ❑ ……...
  - ❑ Other Countries: ..…….
  ……

4 **What type of conditional access device[103] do you develop and sell?** (Several answers possible)

- ❑ Password system
- ❑ Encrypting system
- ❑ Evaluation and filtering system
- ❑ System based on biometrics
- ❑ Other/s?……..
- ❑ ……...……..
- ❑ ……...……..

5 **For what type of services do you develop conditional access?** (Several answers possible)

- ❑ Television broadcasting services
- ❑ Radio broadcasting services
- ❑ Information society services[104] (please specify what sort of service)……

……..

- ❑ Other/s:...…….

……..

6 **What are the areas of application for the devices that you develop?**

- ❑ Economic sectors (Please briefly explain)..…….

……...

……...

……..

- ❑ Activity sectors (Please briefly explain)..…...……..

……...

……...

……..

7 **What will the device/s that you develop be used for?** (Several answers possible)

- ❑ To ensure payment of services
- ❑ Targeted distribution of services
- ❑ Identification of users
- ❑ Collecting information
- ❑ Data protection
- ❑ Property protection, e.g. intellectual property rights
- ❑ Security of communication
- ❑ Protection of firm-owned soft-/hardware (internal infrastructure)
- ❑ Security of commercial transactions
- ❑ To comply with legal/contractual obligations
- ❑ Other/s: (Please briefly explain)..……
- ❑ …….

……..

……..

[103] Conditional access device means any equipment or software designed or adapted to give access to a protected service in intelligble form.

[104] Information Society Service means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

ECONOMIC IMPACT OF CONDITONAL ACCESS DEVICES

8 **What is your estimation of the world market revenue from the supply of conditional access devices?**

…….....
…….....
……...

- Of this figure, what is the European Union's share?

……..…….

- Of this figure, what is North America's share?

……..

9 **How do you view the perspective of growth of this market in the medium term (in %)?**

- World-wide……
- European Union…..…….
- North America ……

10 **What are the economic/activity sectors that will drive this market?**

- Administration (local government?)
- Banking - Insurance
- Transport - Tourism
- Media - Telecoms
- Medicine
- Other/s, namely:...……..……..
- Other/s, namely: ..……..……..
- Other/s, namely: ..……..……..
- …….

THE PROBLEM OF ILLICIT ACCESS TO CONDITIONAL ACCESS SERVICES

11 How do you rate the vulnerability of conditional access devices serving non-remuneration reasons to piracy?

- Very high
- High
- Medium
- Low
- No
- If yes: For which particular reason/s are the pirated device implemented (see e.g. the list in question 7)?…..……

…….……..
……..

12 **Please briefly explain the forms of piracy involved in.** (Please indicate what is correct)

- ❑ Manufacture/ import/ distribution/ sale/ rental/ possession for commercial purposes of illicit devices[105]
- ❑ Installation/ maintenance/ replacement for commercial purposes of an illicit device
- ❑ Use of commercial communication to promote illicit devices
- ❑ Use/possession of illicit devices for commercial purposes
- ❑ Use/possession of illicit devices for private purposes
- ❑ Other/s:...…..……...
- ❑ …….

13 **What are the consequences of piracy of conditional access devices for non-remuneration reasons to your activity?** (Several answers possible)

- ❑ Loss of income
- ❑ Loss of credibility/confidence
- ❑ Loss of clients
- ❑ Higher costs/time needed to develop new systems
- ❑ Legal consequences (e.g. legal actions)
- ❑ Other/s: ……..……..
- ❑ ……..……
- ❑ ……..……

Can you specify the amount of damage suffered (in Euro)? ……..……..

SOLUTIONS PROVIDED BY NATIONAL LAWS

14 **Do you consider the existing national legal protection of conditional access devices which serve non-remuneration interests appropriate and sufficient?**

- ❑ No
- ❑ Yes

Please explain your reasons:..……..
……..
……..
……...
……...
……..
……..
……..
……..
……..
……..
……..
……..……

[105] Illicit device shall mean any equipment or software designed or adapted to give access to a protected service in an intelligible form without authorisation of the service provider.

15 **If you do not consider the existing protection sufficient, does the absence of efficient legal protection of conditional access devices affects the activity of your organisation?**

- ❑ No
- ❑ Yes (Please briefly explain)……...

……...
……...
……...
……..
……..
……..
……...

THE OPERATION OF THE INTERNAL MARKET: OBSTACLES TO THE FREE MOVEMENT OF CONDITIONAL ACCESS DEVICES

16 **Does absence/disparity of legal protection of conditional access devices in other countries affect the activity of your organisation?**

- ❑ No
- ❑ Yes: (Please briefly explain)…..……...

……...
……...
……...
……..
……..
……...

17 **To what extent does the level of legal protection of conditional access devices affect your negotiation position with respect clients?**

- ❑ To a considerable amount
- ❑ To some extent
- ❑ Not

18 **Have you experienced any particular problems in the manufacture, importing and marketing of conditional access devices in a country of the European Union as a result of national laws in force on the legal protection of conditional access devices?**

- ❑ No
- ❑ Yes (Please briefly explain and indicate in which country/ies)……...

……
……..
……..
……..
……..
……..
……..
……..

NEED FOR ADDITIONAL LEGAL PROTECTION

19 **Are you of the opinion that additional legal protection for conditional access devices serving non-remuneration interests is needed?**

- ❑ No
- ❑ Yes

20 **Which general reasons for using conditional access devices require protection?**

- ❑ Remuneration interests
- ❑ Secrecy and confidentiality of communication
- ❑ Data protection
- ❑ Secrecy and confidentiality of information
- ❑ Intellectual property rights
- ❑ Security of infrastructure
- ❑ Security of financial transactions
- ❑ Economic interests of the service/content providers (e.g. targeting markets, collecting information, controlling access to contents, ensuring exclusivity etc.)
- ❑ Other interests: (Please briefly explain which)……..……...
- ❑ ……..
- ❑ ……...
- ❑ No distinction is to be made between the reasons conditional access devices serve.

21 **What sanctions/remedies are needed?**

- ❑ Monetary fines
- ❑ Prison sentences
- ❑ Administrative provisions
- ❑ Civil provisions: (Please briefly explain)……..

…….....…….

…….

Space for further remarks: ……
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...
……...

……..
……..
……..

Please send your reply to:
Institute for Information Law (IViR)
Ms Natali Helberger
Rokin 84
NL-1012 KX Amsterdam

or:
fax: + 31 20 525 3033
or:
e-mail: helberger@jur.uva.nl