RECOMMENDATIONS

OF THE EUROPEAN PROJECT - DIGITAL VIDEO BROADCASTING

ANTIPIRACY LEGISLATION FOR DIGITAL VIDEO BROADCASTING

October 1995

EXECUTIVE SUMMARY

The European Project - Digital Video Broadcasting recommends that the European Union adopt a directive which can attack audiovisual piracy in digital video broadcasting. Based on a report of its Task Force on Antipiracy Legislation, the DVB Project has found that such a directive could be modelled on the Recommendation of the Council of Europe which provides for legal protection for encrypted television services. The Recommendation is suitable for attacking today's analogue audiovisual piracy. In the digital environment, a directive should also address

the quantitative increase in the forms of audiovisual piracy;

the standardization of DVB consumer equipment; and

the introduction of new media services beyond classic broadcasting.

Some further changes could be introduced in the directive which reflect the experiences in Europe fighting audiovisual piracy. Most notably: criminalization of possession of pirate decoders and customs control made more effective.

Adopted in 1991, the Recommendation of the Council of Europe prohibits -- with penal, administrative and civil sanctions -- the manufacture, importation, distribution, commercial promotion and advertising, and possession of decoding equipment

> designed to enable access to an encrypted service by those outside the audience determined by the encrypting organisation.

"Decoding equipment" is defined as any device, apparatus or mechanism designed or specifically adapted to enable access in clear to an encrypted service.

As part of a number of measures adopted in September 1994 on conditional access, the Steering Board of the DVB Project declared that adequate legislation against piracy is a necessary complement to technical security measures. The Task Force on Antipiracy Legislation was formed to make specific recommendations on antipiracy legislation to the Steering Board. The Task Force, composed of members of the DVB Project, also reviewed existing antipiracy laws in many countries within Europe.

Adopted by its Steering Board at its meeting on 7 March 1995, the recommendations of the DVB Project are part of the advice to public authorities, including the European Commission, on the regulatory needs to facilitate the aims and objectives of the DVB Project. The recommendations are a contribution to the official policy framework that removes obstacles to a market-led and consumer-oriented introduction to a digital video broadcasting service in Europe.

The report submitted by the Task Force contains its Recommendations, an Explanatory Memorandum and, as appendices, copies of the Recommendation of the Council of Europe, the survey of laws adopted in the several countries within Europe and the Study, prepared by Kornmeier & Schardt, Rechtsanwalte, on Measures against Piracy of Encrypted Programmes. A copy of the full report including the survey and Study can be obtained from the DVB Project Office.

RECOMMENDATIONS

The Steering Board of the European Project - Digital Video Broadcasting recommends that

1. the European Union adopt a directive modelled after Recommendation No. R (91) 14 of the Council of Europe on the legal protection of encrypted television services

   modified to take account of new factors in digital video broadcasting:

   a. the directive should be a constraining instrument applied across the European Union to ensure that there are no longer any "low-protection" countries;

   b. the sanctions, including penal sanctions, for audiovisual piracy should be sufficiently onerous to discourage commercial pirates;

   c. the definition of "Encrypted service" contained in the Recommendation should be broadened to extend protection to new media services; and

   d. confirmation that the protections within the European Union against counterfeit goods (notably Council Regulation (EC) No 3295/94 of 22 December 1994 laying down measures to prohibit the release for free circulation, export, re-export and entry for a suspensive procedure of counterfeit goods) are applicable against pirate decoders;

   and further modified to reflect the experience within Europe of application of the Recommendation:

   e. personal possession of pirate digital decoders should be criminalized;

2. the European Commission and other institutions of the European Union include the directive referred to in paragraph 1 as a measure to be adopted by PECO states for the purpose of

   > improv[ing] the protection of intellectual, industrial and commercial property rights in order to provide . . . a level of protection similar to that existing in the Community, including comparable means of enforcing such rights

   under the respective Europe Agreements with such states (for example, Europe Agreement with Poland, art. 66(1), O.J. L 348/17 (31 Dec. 1993)); and

3. the Council of Europe continue its efforts to encourage adoption of the Recommendation by its member states and consider modification of the Recommendation consistent with paragraph 1.

EXPLANATORY MEMORANDUM

1. INTRODUCTION.

Within Europe, audiovisual pirates are already capable of attacking the technical measures taken by pay television services to protect today's analogue television signals. In response, pay operators (and those supplying conditional access services) improve their encryption systems to counteract the "hacking" of decoders. They also use legal means -- both criminal and civil -- to stop the activities of pirates or to make them commercially unattractive. The countries of Europe today have a patchwork of laws against pirates. Some are based on the Recommendation of the Council of Europe[1]. In other countries, there is no express protection, for example in Germany and in many states of central and eastern Europe. Other legal theories may be available to prosecute claims.[2]

Pay operators and conditional access providers believe that the Recommendation is generally satisfactory as a measure to combat today's audiovisual piracy. The Recommendation could be improved in the light of experience.

Digital video broadcasting will present new challenges for combating audiovisual piracy.

The Task Force on Antipiracy Legislation of the European Project - Digital Video Broadcasting was asked to make recommendations on the legal measures needed to combat audiovisual piracy. The DVB Project has found that such measures are needed as a necessary complement to technical security measures. These technical security measures include the common scrambling algorithm to be specified by the DVB Project for digital video broadcasting.

2. COUNCIL OF EUROPE RECOMMENDATION.

In 1991 the Council of Europe adopted the Recommendation on the legal protection of encrypted televisions signals. Since then it has been used as the basis for antipiracy laws in several countries within Europe. The Recommendation is an attractive model for national laws

---

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 signals

2 For example, for claims based on laws relating to unfair competition; telecommunications; copyright, patent, trademark and other intellectual property; software protection; and customs.

because its efficacy has already been demonstrated and it is addressed to all the member states of the Council of Europe (a wider group than the 15 Member States of the European Union).[3]

The Recommendation is also attractive because it is easy to understand and to apply. It is an instrument which the police can easily enforce because it addresses a well-defined object -- the pirate decoder -- and its manufacture, importation, distribution, commercial promotion and advertising and possession. Other legal theories could require more complex offers of proof in order to obtain a seizure of illegal decoders or a criminal conviction.

The Task Force considered in what way the Recommendation should be modified to take account of the novel factors which will arise in digital video broadcasting.

3. SPECIAL CONSIDERATIONS FOR DVB.

The Task Force identified three factors which should be addressed in any measure to combat piracy in digital video broadcasting:

a. The Task Force concluded that there will be a quantitative increase in the forms of audiovisual piracy described in Recommendation. There will be more pay, encrypted audiovisual services; the aggregate number of subscribers will increase throughout Europe; the installed base of decoders will grow substantially. As the market for pay services grows, the manufacture, distribution and marketing of pirate decoders will become commercially more attractive.

   One lesson to be drawn from this conclusion is that a instrument more constraining than the Recommendation is needed. The Recommendation is in the nature of a model law. What is required is an instrument like a directive of the European Union addressed to its Member States.[4]

b. A second conclusion drawn by the Task Force is that the availability of standardized DVB equipment throughout Europe will make cross-border piracy more feasible. The DVB Project has proposed specifications for digital video broadcasting. These specifications will be implemented into DVB consumer equipment, including IRDs and decoders. Among the specifications is a common scrambling system.

---

[3] Within the European Union, piracy matters were initially linked to the Commission's work on copyright, Green Paper on copyright and the challenge of technology, COM (88) 172 (7 June 1988), but then postponed at the time the Commission began work on its directive on copyright for cable and satellite transmissions. Broadcasting and copyright in the internal market: Discussion paper prepared by the Commission of the European Communities on copyright questions concerning cable and satellite broadcasts, s. 5.3.2 (Nov. 1990).

[4] Of course, the Council of Europe should continue its efforts to encourage Member States to adopt antipiracy legislation following the model of Recommendation. Indeed, the Council should consider adopting further more constraining instruments.

The adoption of the common scrambling system across Europe increases the commercial attractiveness of attacking the system. More pirates will attempt to "hack" the system. Because DVB consumer equipment will be standardized, it is possible for pirate IRDs and decoders,[5] manufactured in one European Member State, to be used in a second. Pirates will manufacture in countries with a low level of antipiracy protection and export to states with higher levels. Moreover, there is the danger of a significant increase in cross-border importation of pirate decoders by individuals for private use in their home country. The problem is enhanced, of course, in the market for DVB services transmitted to the consumer by satellite.

From this conclusion, it is apparent that there is need for harmonized rules across Europe to limit cross-border piracy. The rules in Europe on counterfeit and pirated goods, contained in a recently adopted Council Regulation, should be applied to pirate decoders.[6] In addition, there should be consideration of stronger rules, indeed criminalization, of possession of pirate decoders even for private purposes.

c. A further conclusion is that the range of DVB services will extend far beyond the passive "couch potato" television services we know today. The standardized DVB consumer equipment may contain many functionalities for new media services, including capacity for interactive services, pay-per-view, video-on-demand and delivery of games.

With this in mind, the definition of "Encrypted service" in the Recommendation should be re-examined. The definition speaks of "television service", that is "intended for direct reception by the general public". The explanatory memorandum accompanying the Recommendation could be changed to take account of these new services. It would be ironic that laws based on the Recommendation would apply to pirate decoders to the extent they enable access to a classic subscriber service, but not in respect of piracy of VOD services offered through the same decoders.

4. *IMPROVEMENTS TO THE RECOMMENDATION.*

Pay operators and conditional access providers already have significant experience applying laws based on the Recommendation in combating audiovisual piracy in analogue television. As a result of that experience, the Task Force on Antipiracy Legislation has found,

---

5 By "decoders" we follow the meaning of Decoding equipment in the Recommendation: "any device, apparatus or mechanism . . . " Thus the Recommendation covers not only a classic decoder box, but also module suitable for a common interface, smart cards, etc.

6 Council Regulation (EC) No 3295 of 22 December 1994 laying down measures to prohibit the release for free circulation, export, re-export or entry for a suspensive procedure of counterfeit and pirated goods, O.J. No. L 341/8 (30 Dec. 1994). Pirated decoders could fall outside the definitions of "counterfeit goods" and "pirated goods" (unless the pirated decoder, for example, uses the trademark of a pay broadcaster).

and the Steering Board recommends, that the measures set out below be included either in the EU directive addressing decoder piracy or as modifications of other EU instruments.

The most important further measure to improve enforcement of antipiracy laws is to criminalize possession of pirate decoders. As noted above, criminalization of possession will discourage the growth in the cross-border market in pirate digital decoders. It will also improve the ability to prosecute cases where it is difficult to prove commercial intent.[7]

There are other areas where amendments to existing laws could help in combating audiovisual piracy: For example, encryption algorithms could be more explicitly protected as software. In addition, sanctions generally could be improved: it is unfortunate that the Recommendation allows for "penal or administrative sanctions". Sanctions should be set at a level appropriate for felonies. This would discourage piracy.[8] Similarly a pay operator harmed by a pirate's actions should be able to recover for its losses based on a copyright level of damages. Finally, broadcasters should be able to find protection against piracy in every Member State of the European Union. In other words, antipiracy legislation in a Member State should not be limited to broadcasters licensed in that state.[9]

---

7 For example, if possession is not a criminal act under an antipiracy law, the defendant may claim that pirate smart cards in his possession were intended for his personal use. How many cards are needed to show commercial intent? What if the defendant has a practice of holding only three cards at any time in his shop? Similarly, a pirate decoder may be installed at the headend of an SMATV system serving an apartment block. Here again commercial intent may be hard to demonstrate, but it is clear that the person installing the pirate decoder should be penalized.

8 For example, the draft German law would impose a fine of only 20,000 DM, characterizing piracy as merely an "administrative offence". In contrast, French law provides for imprisonment of up to two years for certain piracy activities.

9 For example, UK legislation against piracy cannot be used by non-UK broadcasters.

DESCRIPTION OF ACTIVITIES OF THE DVB TASK FORCE ON ANTIPIRACY LEGISLATION

The Task Force on Antipiracy Legislation of the DVB Project was formed in May 1994 by decision of the Ad-hoc Group on Conditional Access. The participants in the Task Force included representatives of pay and commercial broadcasters and conditional access suppliers. Carter Eltzroth of FilmNet was named as chairman.

The Task Force surveyed legislation existing and proposed in Europe to combat audiovisual piracy. Because of the scope of this work, the DVB Project, upon the recommendation of the Task Force, engaged as special counsel Andreas Schardt of Kornmeier & Schardt, Rechtsanwalte, Frankfurt.

The Task Force reported on its progress to the Steering Board and to the Ad-hoc Group on Conditional Access, most recently on its conclusions at the Ad-hoc Group's meeting on 16 February 1995. Its report was adopted by the Steering Board of the DVB Project on 7 March 1995.

The Steering Board is grateful to the ministries of Member States and to others for furnishing copies of their antipiracy legislation. These are available from the DVB Project Office.

APPENDICES

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 signals

2. Survey of European national antipiracy legislation*

3. Study, prepared by Kornmeier & Schardt, Rechtsanwalte, on Measures against Piracy of Encrypted Programmes*

* Not included. Available from the DVB Project Office.

APPENDIX 1

Council of Europe
Conseil de l'Europe

The legal protection of encrypted television services

Recommendation No. R (91) 14
and explanatory memorandum

Mass media

The legal protection of encrypted television services

Recommendation No. R (91) 14
adopted by the Committee of Ministers
of the Council of Europe
on 27 September 1991
and explanatory memorandum

Council of Europe Press, 1995

French edition:
La protection juridique des services de télévision cryptés (Recommandation n° R (91) 14)
ISBN 92-871-2709-3

Publishing and Documentation Service
Council of Europe
F-67075 Strasbourg Cedex

ISBN 92-871-2710-7

Printed at the Council of Europe

1. Recommendation No. R (91) 14, adopted by the Committee of Ministers of the Council of Europe on 27 September 1991, was prepared by the Steering Committee on the Mass Media (CDMM).

2. This publication contains the text of Recommendation No. R (91) 14 and the explanatory memorandum prepared by the CDMM.

Recommendation No. R (91) 14

of the Committee of Ministers to member states on the legal protection of encrypted television services

(Adopted by the Committee of Ministers on 27 September 1991 at the 462nd meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage and facilitating their economic and social progress;

Noting the increasing development in Europe of television services, notably pay-TV services, the access to which is protected by means of encryption techniques;

Taking into account that these services contribute to the diversity of television programmes offered to the public and, at the same time, increase the possibilities of exploitation of audiovisual works produced in Europe;

Considering that the development of pay-TV is likely to increase the sources of financing of television services and, as a result, the capacities of audiovisual production in Europe;

Concerned by the increasing degree of illicit access to encrypted television services, namely, access by persons outside the audience for which the services are reserved by the organisation responsible for their transmission;

Noting that this phenomenon is such as to threaten the economic viability of organisations providing television services and, hence, the diversity of programmes offered to the public;

Taking into account the fact that illicit access to encrypted television services also threatens the legal certainty in the relations between, on the one hand, the organisations providing encrypted television services and, on the other hand, holders of rights in works and other contributions transmitted in the framework of such services;

Being aware that illicit access to encrypted television services indirectly prejudices the rights and interests of authors, performers and producers of audiovisual works, as well as of the cultural professions and related industries as a whole;

Noting that the organisations providing encrypted television services have the responsibility to use the best available encryption techniques;

Recognising nevertheless that legislative action is needed to supplement such techniques;

Determined that effective action should be taken against illicit access to encrypted television services;

Believing that this can most effectively be achieved by concentrating on commercial activities enabling such access;

Recognising that the protection of encrypted television services in domestic legislation should not be subject to the requirement of reciprocity,

Recommends the governments of the member states to take all necessary steps with a view to implementing the following measures to combat illicit access to encrypted television services :

Definitions

For the purpose of the implementation of Principles I and II hereafter :

"encrypted service" means any television service transmitted or retransmitted by any technical means, the characteristics of which are modified or altered in order to restrict its access to a specific audience;

"decoding equipment" means 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 modification or alteration of its characteristics;

"encrypting organisation" means any organisation whose broadcasts, cable transmissions or rebroadcasts are encrypted, whether by that organisation or by any other person or body acting on its behalf;

"distribution" means the sale, rental or commercial installation of decoding equipment, as well as the possession of decoding equipment with a view to carrying out these activities.

States should include in their domestic legislation provisions based on the principles set out hereafter :

Principle I – Unlawful activities

1. The following activities are considered as unlawful :

a. the manufacture of decoding equipment where manufacture is designed to enable access to an encrypted service by those outside the audience determined by the encrypting organisation;

b. the importation of decoding equipment where importation is designed to enable access to an encrypted service by those outside the audience determined by the encrypting organisation, subject to the legal obligations of member states regarding the free circulation of goods;

c. the distribution of decoding equipment where distribution is designed to enable access to an encrypted service by those outside the audience determined by the encrypting organisation;

d. the commercial promotion and advertising of the manufacture, importation or distribution of decoding equipment referred to in the above paragraphs;

e. the possession of decoding equipment where possession is designed, for commercial purposes, to enable access to an encrypted service by those outside the audience determined by the encrypting organisation.

2. However, as regards the possession of decoding equipment for private purposes, member states are free to determine that such possession is to be considered as an unlawful activity.

Principle II – Sanctions and remedies

Principle II.1 – Penal and administrative law

1. States should include in their domestic legislation provisions indicating that the following activities are the subject of penal or administrative sanctions :

a. the manufacture of decoding equipment as prohibited by Principle I.1.*a*;

b. the importation of decoding equipment as prohibited by Principle I.1.*b*;

c. the distribution of decoding equipment as prohibited by Principle I.1.*c*;

d. the possession of decoding equipment where possession is designed, for commercial purposes, to enable access to an encrypted service by those outside the audience determined by the encrypting organisation.

2. Sanctions provided for by legislation should be set at an appropriate level. States should provide for enforcement of these sanctions and, in so far as domestic legislation permits:

a. provision should be made for powers to search the premises of persons engaged in the acts mentioned in paragraph 1 above and to seize all material of relevance to the investigation, including the decoding equipment, as well as the means used for its manufacture;

b. provisions should exist for the destruction or forfeiture of the decoding equipment and of the means used for its manufacture seized in the course of a procedure;

c. the forfeiture of financial gains resulting from the manufacture, importation and distribution activities considered as unlawful in accordance with Principle I should also be possible. In accordance with domestic law, courts should be able to award all or part of any financial gains so forfeited to injured persons by way of compensation for the loss which they have suffered.

Principle II.2 – Civil law

1. States should include in their domestic law provisions which provide that the injured encrypting organisation may, apart from the

proceedings foreseen under Principle II.1, institute civil proceedings against those engaged in activities considered as unlawful in accordance with Principle I, notably in order to obtain injunctions and damages.

2. In so far as domestic law permits, the injured encrypting organisation should, as an alternative to an action for damages in respect of the loss which it has suffered, have the right to claim the profits made from the prohibited activities.

3. In so far as domestic law permits, provision should be made for the seizure, destruction or delivery to the injured encrypting organisation of decoding equipment and the means used for its manufacture.

4. Effective means should exist for obtaining evidence in cases involving the prohibited activities.

Explanatory memorandum

Introduction

1. Broadcasters have traditionally sought to reach the widest possible audience for their programmes. However, following economic and technical developments in recent years in the broadcasting sector, especially the advent of pay-TV services, this is no longer invariably the case, and certain broadcasters now wish to ensure that their audience is restricted. This may be for various reasons. As regards pay-TV services, the broadcaster seeks to restrict the access to its programmes solely to persons paying the required subscription, and the fees paid are used to finance the broadcaster's activities. A broadcaster may also wish to restrict the audience of its programmes for other reasons. For example, it may wish to limit the access to its broadcasts for reasons of copyright and neighbouring rights. Furthermore, particularly in the case of services with a professional vocation, the broadcaster may wish to restrict the access to its programmes to a closed user group particularly interested in the broadcasts (for example, a broadcaster transmitting medical programmes will reserve their access to medical personnel).

2. In order to control the access to its broadcasts, the broadcaster can modify or alter their characteristics by encrypting or encoding them or by using other technical processes such as scrambling techniques, and provide decoding equipment to the specific audience it seeks to address. Although the modified transmission may be widely receivable, only those who have decoding equipment can transform the transmission so that the programme can be seen and heard on the television set. This technical method of controlling the access to television services is highly effective, provided that only those members of the public whom the broadcaster seeks to reach are capable of decoding the signal.

3. Experience has shown, however, that the ability to decode the encrypted broadcast is not confined to the intended audience because decoding equipment capable of decoding the broadcast is made available to those outside the intended audience. This may be pirate decoding equipment, made with the intention of supplying it to persons outside the intended audience, or legitimate decoding equipment which finds its way into the hands of persons who are not entitled to have it.

4. Illicit access to an encrypted television service by persons outside the intended audience clearly has adverse effects on the broadcaster concerned and, indirectly, on the right holders in the works and other contributions which are transmitted in the framework of that service. The most obvious example is the fact that illicit reception enables avoidance of the payment to pay-TV channels of the subscription which they impose for access to their programmes. Moreover, illicit access to an encrypted television service may prejudice the interests of broadcasters other than the broadcaster directly concerned. Illicit access to the programmes of a broadcaster intended for a determined audience may cause the audience of another broadcaster to turn to the programmes of the first broadcaster, in particular if both broadcasters transmit similar programmes.

5. By depriving broadcasters (and thus, indirectly, right holders) of the payments which they are entitled to receive, illicit access to encrypted television services may threaten the economic viability of the broadcasting organisations concerned and, hence, the diversity of programme services offered to the public.

6. Furthermore, even in cases where a programme service is not encrypted for financial reasons but with a 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. The broadcaster whose programmes are received illicitly may expose himself to legal action from right holders 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 right holders.

7. It is thus necessary to consider the action which should be taken in order to dissuade or prevent illicit access to encrypted television services.

8. At first sight, the notion of illicit access, finding expression in the illicit reception of an encrypted television service, is not one that sits comfortably with the principle of freedom of expression and of free access to information enshrined in many national laws and international conventions. For example, Article 4 of the European Convention on Transfrontier Television indicates that the Parties to the convention "shall guarantee freedom of reception" of transfrontier television programme services. However, further reflection reveals 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. Opinions received by the Council of Europe from broadcasters, right holders and manufacturers of decoding equipment have confirmed unanimously the importance of the prejudice which they suffer due to illicit reception. As indicated previously, the practice will, if allowed to continue unchecked, have an adverse effect on investments in broadcasting which will be against the public interest, reducing consumer choice and access to a wider range of television services. Seen from this perspective, illicit reception prejudices the very freedom of reception that Article 4 of the European Convention on Transfrontier Television seeks to ensure.

9. It is apparent from the evidence received by the Council of Europe that technology cannot provide a complete answer to the problems experienced by broadcasters in respect of illicit access to their encrypted television services. Although encryption techniques already provide important security and will continue to be improved, it will always be possible (at least for the foreseeable future) for a person determined to do so to produce illicit decoding equipment to enable access to an encrypted television service. Hence, this justifies the introduction of some legal provisions to reinforce the protection against illicit access to encrypted television services afforded by technology.

10. Therefore, this recommendation invites member states to take certain measures in order to combat illicit access to encrypted television services. It is only concerned with the illicit access to encrypted television services by means of decoding equipment and not with other forms of access to television services which may be regarded as illicit, for example,

reception by members of the public who have not paid a television licence fee. Nor does this recommendation deal in depth with the problem of the retransmission of a signal that has been received illicitly. Indeed, it is to be noted that such activity is already addressed by such international instruments as the Berne Convention for the Protection of Literary and Artistic Works and the Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations, the European Agreement on the Protection of Television Broadcasts and the Brussels Convention relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite.

11. Although the problem of illicit access is posed mainly from the point of view of broadcasting services, it may also concern, more generally, all kinds of distribution of television programmes. The principles set out in this recommendation thus also apply to all kinds of distribution of encrypted television services, for example, by hertzian waves, cable or through multi-point microwave distribution systems.

12. It is clear that the organisation providing an encrypted television service should do all it can to deter illicit access to that service, and to this end should employ the best encryption techniques which are available to it. However, as noted above, this will not always be sufficient and, as has already been recognised in certain member states of the Council of Europe, some legal provisions are needed in order to supplement technical means of protection. In this perspective, this recommendation envisages the enactment of legal provisions in five areas: the manufacture of decoding equipment, the importation of decoding equipment, the distribution of decoding equipment, commercial promotion and advertising of such activities and the possession of decoding equipment. The adoption of legal measures in respect of commercial activities is aimed at guaranteeing the effectiveness of the fight against illicit access to encrypted television services by stopping the circulation of decoding equipment at the source.

Definitions

13. For the purpose of the implementation of this recommendation, a number of definitions are set out which are aimed at clarifying several notions which might give rise to interpretation.

14. "Encrypted service" means any television service transmitted or retransmitted by any technical means, the characteristics of which are modified or altered in order to restrict its access to a specific audience. As noted in the introduction, a variety of techniques may be used to modify or alter the characteristics of a particular encrypted television service (coding, scambling, etc.). The definition also covers all kinds of technical means used for transmitting or retransmitting encrypted programmes, in particular by hertzian waves, including by satellite or multi-point microwave distribution systems, and by cable. On the other hand, it does not apply to the mere transport of signals not intended for direct reception by the general public. The unauthorised interception of such signals, whether encrypted or not, is prohibited under telecommunications law (ITU Radio Regulations). Moreover, the term "encrypted service" and, accordingly, this recommendation, do not apply to television services, the characteristics of which are modified involuntarily, for example due to interferences during their transmission.

15. "Decoding equipment" means 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 modification or alteration of its characteristics. Thus, this definition refers to all kinds of equipment enabling the viewer to receive "in clear" an encrypted service without the modification or alteration made to the signal by the organisation providing the service, although it is not necessary that the quality of the reception be identical to that of the original signal. It covers first the most frequent cases where a decoder in itself enables access to an encrypted service. It also applies to cases where access is only possible if the decoder is coupled with other pieces of equipment or devices. Such is the case when a decoder can only be activated by means of a smart card which provides the key for access to an encrypted programme or transmission. In so far as possible, member states should ensure in this case that the provisions of their domestic legislation adopted under this recommendation only apply to the part of the decoding equipment which in fact provides access to an encrypted service. Finally, the definition also covers cases where a single piece of equipment provides various functions, one of them being to provide access to an encrypted service.

16. "Encrypting organisation" refers to any organisation whose broadcasts, cable transmissions or rebroadcasts are encrypted, whether by that organisation or any other person or body acting on its behalf. Indeed, there might be cases where the technical activity of encryption or coding or scrambling is not directly carried out by the organisation providing the encrypted television service but by a third party with particular competence in this field. Accordingly, this definition covers cases where encryption is provided by a person or body acting on behalf of the organisation providing the encrypted television service.

17. It is to be noted that this definition and, accordingly, the protection provided by this recommendation apply to all the organisations offering encrypted television services, both at local or regional level and at national and transfrontier level. Moreover, the protection applies regardless of the nationality of the organisations, and regardless of whether or not they come under the jurisdiction of the member states of the Council of Europe. Furthermore, the protection is not to be made subject to any requirement of reciprocity in the national legislations concerned.

18. Indeed, if member states were to grant protection only on a reciprocal basis, this could disadvantage right holders whose works or contributions are included in a non-protected broadcast. Furthermore, by excluding a foreign television organisation from such protection, a state might prejudice its own national television organisations: as mentioned previously, the illicit access of its public to the programmes of a foreign television organisation could result in the public neglecting the programmes of its own national television organisations. For these reasons, this recommendation calls for protection of all organisations providing encrypted television services irrespective of their nationality.

19. "Distribution" covers all commercial activities relating to the supply of decoding equipment to the public, from wholesale to retail or rental. It also takes into account the commercial installation of decoding equipment, such as the installation of decoding equipment in an individual's home.

Principle I – Unlawful activities

Manufacture

20. If an organisation providing a television service wishes to limit its audience by the use of an encryption technique, it must not only encrypt the broadcast which it transmits but also ensure that decoding equipment is manufactured to supply the public it wishes to reach. Since such decoding equipment is frequently sold or leased to the public and provides the mechanism for payment for the service, unscrupulous manufacturers might be tempted to produce decoding equipment for sale at a price which need take no account of the payment for the television service and, hence, is much cheaper than the decoding equipment supplied lawfully. Although it is not covered by copyright law, this activity is not dissimilar in either its motivation or effect to copyright piracy, where protected works are reproduced for commercial purposes without the consent of the owner of the rights. The manufacture of such pirate decoding equipment is prejudicial to the interests of organisations providing encrypted television services and, indirectly, of the right holders in works and other contributions incorporated in encrypted services in much the same way as the production of infringing copies is prejudicial to copyright interests.

21. The analogy with copyright is not, however, a complete one. Whilst it is quite appropriate for legislative measures to be introduced against those who manufacture infringing copies without the authorisation of the right holders, it does not seem appropriate to legislate against the manufacture of decoding equipment which is done without the consent of the organisation whose encrypted services can be received through this equipment. Not only would this appear to create some new form of property right in the decoding equipment, but it could deter electronics companies from research and development in this field, since they could expose themselves to legal action if they made decoding equipment without some prior authorisation from the encrypting organisation. This difficulty would be particularly noticeable in the case where decoding equipment invented by a manufacturer would enable access to different encrypted television services and would only be authorised by one or some of the organisations providing such services; both the manufacturer and these organisations would be in a state of total uncertainty as to actions which the organisation(s) which

has (have) not given permission could bring. A simple prohibition on making decoding equipment without the authority of the encrypting organisation would thus prevent a manufacturer from producing a new encryption system which it wished to develop first and then find an organisation providing an encrypted television service to buy it. This would act as a brake upon the development of more effective encryption techniques and run counter to the interests of organisations providing encrypted television services.

22. The manufacturer who merits censure is the one who makes decoding equipment for supply to an audience outside the one to which the encrypting organisation intends to reserve its encrypted television service. This recommendation therefore considers as unlawful the manufacture of decoding equipment where manufacture is designed to enable illicit access to an encrypted service.

Importation

23. Importation of decoding equipment may be at the source of its circulation within a given country. Manufactured or distributed, even legally, in one country, it may be imported into another country and subsequently distributed so as to enable access in that country to an encrypted service by those outside the audience determined by the encrypting organisation. Accordingly, and given the crucial role which the customs authorities may play in combating the illicit circulation of decoding equipment, this recommendation considers as unlawful the importation of decoding equipment where it is designed to enable illicit access to an encrypted service. Some countries have already provided for prohibitions on the importation of decoding equipment where importation is designed to enable television viewers to have illicit access to encrypted television services. Principle I.1.*b* advocates a similar approach. However, as regards European Community member states, the decision to regard importation as a prohibited activity is not to be seen as prejudicing the operation of the relevant provisions of the Treaty of Rome on the free movement of goods, including the decisions of the Court of Justice of the European Communities in regard to the meaning of those provisions. Accordingly, the recommendation provides that the decision to consider the importation of decoding equipment as an unlawful activity, as mentioned in Principle I.1.*b*, must be without prejudice to the legal obligations of member states regarding the free

circulation of goods. It should also be borne in mind that the recommendation is addressed not simply to the governments of the community states which are member states of the Council of Europe but to all member states of the Council of Europe, thirteen of which are not bound by the Treaty of Rome's provisions on free movement of goods. Thus, it was felt appropriate to give such countries guidance on how to deal with the issue of importation of decoding equipment for the purposes described in Principle I.1.*b*.

Distribution

24. Although measures aimed at the manufacture of decoding equipment will go some way towards preventing the problems of illicit access to encrypted services, it is clear this will not be sufficient. In order to make the fight against illicit access to encrypted television services really effective, it is also necessary to sanction the whole range of activities relating to distribution, which are designed to enable unlawful access. As indicated in the definitions above, this recommendation covers the whole chain of operations ranging from wholesale distribution to retail sale or rental, including the illicit sale or rental of decoding equipment and the commercial installation of decoding equipment.

Commercial promotion and advertising

25. Since the manufacturers, importers and distributors of decoding equipment may decide to promote their activities, this recommendation provides, in order to complete the range of means available against illicit access to encrypted television services, that it is also unlawful to commercially promote and advertise the manufacture, importation and distribution of decoding equipment considered unlawful in application of Principle I. Thus, Principle I.1.*d* not only applies to advertising in the classic sense of the term in favour of the aforementioned activities, but also to any practice related to advertising which is designed to promote the same activities (sponsorship, etc.). This recommendation envisages only civil remedies, for example, in the form of injunctions, in order to stop activities in the area of commercial promotion and advertising which are prohibited. Moreover, it should be noted that sanctions likely to be taken should be aimed exclusively at manufacturers, importers and distributors of decoding equipment and not at organisations which

create or carry material used for commercial promotion or advertising (advertising agencies, newspapers, magazines, etc.).

26. This recommendation does not prohibit the publication of technical information enabling access to an encrypted television service, in so far as it does not constitute a form of advertising or commercial promotion of the prohibited activities. Such a ban might indeed run counter to the principle of freedom of information, as established under certain domestic legislation. However, those member states which consider it possible to ban such publication on the grounds that it commercially promotes or advertises a prohibited activity, and which judge such a ban useful, may adopt provisions to this effect.

Possession

27. When a member of the public uses decoding equipment to receive an encrypted television service to which he is not entitled to have access, he will deprive the encrypting organisation concerned of the control which encryption was intended to provide. At the very least, he damages the organisation by putting it to useless expense, but more usually he will be defrauding it of the payment that is due to it and this will indirectly prejudice the interests of right holders in the works and other contributions included in the television service.

28. The recommendation makes a distinction between possession for commercial purposes and possession for private purposes in order to take into account that the adoption of provisions which seek to regulate what is done in the privacy of the home for purely non-commercial purposes could raise difficulties in regard to the right to private life embodied in certain national legislation. On this account, certain member states might find it impossible to provide remedies, both penal and administrative as well as civil, against the possession of decoding equipment for private purposes. Moreover, such provisions may be difficult to enforce. On the one hand, detection is *a priori* virtually impossible and even when the activity is detected, there may be practical difficulties in enforcing the law. Indeed, enforcement can be seen by the general public as heavy-handed and may bring the law itself into disrepute. For this reason, the recommendation does not deal with possession of decoding equipment for private purposes while providing

that member states are free to determine that such possession is to be considered as an unlawful activity.

29. Sanctions against the illicit use of decoding equipment by an individual can nevertheless contribute towards dissuading such use, even though their application may prove difficult. Thus, member states which consider it desirable to introduce remedies against illicit access to encrypted television services by individuals may do so. Those states could usefully refer on the subject to the provisions already set out in certain national laws.

30. It should also be borne in mind that decoding equipment may be used to enable a sizeable audience, outside the one determined by the encrypting organisation, to have access to an encrypted service, for purposes other than commercial ones. For example, it may be the case that an individual enables his co-residents of a block of flats sharing a collective antenna to have access to encrypted television services by using decoding equipment in his possession. The aim of the individual is not to gain a financial advantage, but to offer a friendly service out of a sense of shared community. However, given the substantial number of persons having illicit access to encrypted television services in this way, member states may feel that it is appropriate to prohibit possession of decoding equipment in such circumstances, even though the motive for use may not be commercially inspired.

31. On the other hand, the illicit use of decoding equipment for commercial purposes should be considered as an unlawful activity, due to the special prejudice this entails for the encrypting organisation which is a victim of such use. Such would be the case, for example, of an hotel proprietor or a cable operator using one or more decoders in order to offer illicit access by his clients to an encrypted television service. In so doing, the hotel proprietor or cable operator does not limit himself to an act of illicit reception but acquires an undue advantage from this activity, by including this service in the bill presented to clients or subscribers.

32. As in the case of private use of decoding equipment, use for commercial purposes may be difficult to prove. Punishing the use of decoding equipment presupposes that the police can record such use. Unless the police catches the user *in flagrante delicto*, it will, in practice,

be impossible to record such use. Therefore, the recommendation sanctions the possession of decoding equipment, with the presumption that such equipment will be used. This presumption is similar to that foreseen in certain domestic legislation which sanctions possession rather than use (for example, as regards the regulation of firearms).

Principle II – Sanctions and remedies

33. Having considered the activities which should be considered as unlawful, the question arises as to what legal measures should be introduced to deal with these activities. As noted previously, there are a number of parallels between the manufacture and distribution of decoding equipment for enabling illicit access to encrypted television services and the making and distribution of infringing copies prohibited by copyright law. In drawing up the provisions of this recommendation relating to sanctions and remedies, the Council of Europe's Recommendation No. R (88) 2 on measures to combat piracy in the field of copyright and neighbouring rights has proved a useful model. However, the fact that a copyright provision was, in this limited respect, taken as a model from which this principle was developed does not imply that this is a matter of copyright law. The measures set out in this recommendation may be implemented in whichever branch of law is deemed to be most appropriate by member states. Among the possibilities are telecommunications law, broadcasting law, administrative law, criminal law and additional provisions in the field of copyright law; these could also be used in combinations or a *sui generis* provision may provide the best solution. There is therefore complete flexibility for member states in their methods of implementation of this recommendation.

34. The recommendation contains both criminal or administrative provisions and civil remedies. Such provisions constitute a minimum framework of intervention. Member states which so wish may therefore adopt stricter regulations than the one envisaged in this recommendation, in particular as regards the determination of activities subject to penal or administrative sanctions.

Penal and administrative provisions

35. The recommendation provides that the manufacture, importation and distribution of decoding equipment in a way which is designed

to enable illicit access to encrypted television services, as well as the possession of decoding equipment for commercial purposes as defined in Principle II.1, are subject to either penal or administrative sanctions. As indicated in paragraph 28, the fact that the possession of decoding equipment for private purposes, as well as advertising and commercial promotion activities, are not considered among the activities subject to penal or administrative sanctions is designed to take account of the fact that certain member states might consider that the provision of such sanctions, and in particular penalties which result in a deprivation of liberty, would be disproportionate or impossible in the context of their national legal system.

36. Penalties should be set at an appropriate level; those provided in national legislation against copyright piracy can constitute a useful reference as to the appropriate level.

37. In so far as the legislation of member states permits, powers of search and seizure should be foreseen in order to obtain the necessary evidence, and the law should provide for the forfeiture of prohibited decoding equipment, as well as for the destruction of pirate decoding equipment and the means used for their manufacture. There should also be the possibility of forfeiting the profits from these illegal activities. If the national law permits, such forfeited profits may be awarded to the persons injured by illicit access to an encrypted television service, namely the encrypting organisation providing the service as well as right holders in works and other contributions transmitted in the framework of the service and received illicitly.

Civil remedies

38. The recommendation also envisages that civil proceedings can be brought against those who engage in any of the prohibited activities. The usual remedies – injunctions, damages – should be available, and, where domestic law so permits, the injured encrypting organisation should also be able to claim, as an alternative to damages, forfeiture of profits made from activities prohibited by virtue of this recommendation. Moreover, in so far as national legislation permits, the injured encrypting organisation should have the possibility of obtaining the seizure, destruction or delivery of decoding equipment and the means used for its manufacture. In so far as member states do not yet have

such machinery, there should be proper machinery in place so that the necessary evidence can be obtained.

39. Although it is not stated expressly, courts should refuse to give effect to contracts or clauses in contracts concerning the manufacture, importation, distribution or any other prohibited activity referred to in this recommendation.

40. Only the organisation which has encrypted a television service has a right of action under this recommendation. Although holders of copyright and neighbouring rights may suffer if illicit access to such broadcast occurs, this damage is indirect. Moreover, if all the right holders were given a right of action it would create the potential for a multiplicity of legal actions. Since it is the encrypting organisation which suffers the direct damage, the legal process will be greatly simplified if that organisation alone has recourse to the courts. The right holders can ensure that their interests are safeguarded by contractually requiring the encrypting organisation to act against illicit access to its encrypted television services. In most cases, the principal concern is to ensure that the activity is stopped and injunctions and seizure may be all that is sought. But if any damages/forfeited profits are awarded to the injured encrypting organisation, the right holders should expect a share which is proportional to the harm they have suffered. This being said, member states are of course at liberty to give specific rights and remedies to aggrieved right holders, for example the right to take legal proceedings against manufacturers, importers or distributors of illicit decoding equipment.

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l'Europe

AUSTRALIA/AUSTRALIE
Hunter publications, 58A, Gipps Street
AUS-3066 COLLINGWOOD, Victoria
Fax: (61) 34 19 71 54

AUSTRIA/AUTRICHE
Gerold und Co., Graben 31
A-1011 WIEN 1
Fax: (43) 1512 47 31 29

BELGIUM/BELGIQUE
La Librairie européenne SA
50, avenue A. Jonnart
B-1200 BRUXELLES 20
Fax: (32) 27 35 08 60

Jean de Lannoy
202, avenue du Roi
B-1060 BRUXELLES
Fax: (32) 25 38 08 41

CANADA
Renouf Publishing Company Limited
1294 Algoma Road
CDN-OTTAWA ONT K1B 3W8
Fax: (1) 613 741 54 39

DENMARK/DANEMARK
Munksgaard
PO Box 2148
DK-1016 KØBENHAVN K
Fax: (45) 33 12 93 87

FINLAND/FINLANDE
Akateeminen Kirjakauppa
Keskuskatu 1, PO Box 218
SF-00381 HELSINKI
Fax: (358) 01 21 44 35

GERMANY/ALLEMAGNE
UNO Verlag
Poppelsdorfer Allee 55
D-53115 BONN
Fax: (49) 228 21 74 92

GREECE/GRÈCE
Librairie Kauffmann
Mavrokordatou 9, GR-ATHINAI 106 78
Fax: (30) 13 83 03 20

IRELAND/IRLANDE
Government Stationery Office
4-5 Harcourt Road, IRL-DUBLIN 2
Fax: (353) 14 75 27 60

ISRAEL/ISRAËL
ROY International
PO Box 13056
IL-61130 TEL AVIV
Fax: (972) 349 78 12

ITALY/ITALIE
Libreria Commissionaria Sansoni
Via Duca di Calabria, 1/1
Casella Postale 552, I-50125 FIRENZE
Fax: (39) 55 64 12 57

NETHERLANDS/PAYS-BAS
InOr-publikaties, PO Box 202
NL-7480 AE HAAKSBERGEN
Fax: (31) 542 72 92 96

NORWAY/NORVÈGE
Akademika, A/S Universitetsbokhandel
PO Box 84, Blindern
N-0314 OSLO
Fax: (47) 22 85 30 53

PORTUGAL
Livraria Portugal, Rua do Carmo, 70
P-1200 LISBOA
Fax: (351) 13 47 02 64

SPAIN/ ESPAGNE
Mundi-Prensa Libros SA
Castelló 37, E-28001 MADRID
Fax: (34) 15 75 39 98

Llibreria de la Generalitat
Rambla dels Estudis, 118
E-08002 BARCELONA
Fax: (34) 34 12 18 54

SWEDEN/SUÈDE
Aktiebolaget CE Fritzes
Regeringsgatan 12, Box 163 56
S-10327 STOCKHOLM
Fax: (46) 821 43 83

SWITZERLAND/SUISSE
Buchhandlung Heinimann & Co.
Kirchgasse 17, CH-8001 ZÜRICH
Fax: (41) 12 51 14 81

BERSY
Route du Manège 60, CP 4040
CH-1950 SION 4
Fax: (41) 27 31 73 32

TURKEY/TURQUIE
Yab-Yay Yayimcilik Sanayi Dagitim Tic Ltd
Barbaros Bulvari 61 Kat 3 Daire 3
Besiktas, TR-ISTANBUL

UNITED KINGDOM/ROYAUME-UNI
HMSO, Agency Section
51 Nine Elms Lane
GB-LONDON SW8 5DR
Fax: (44) 718 73 82 00

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Company
468 Albany Post Road
PO Box 850
CROTON-ON-HUDSON, NY 10520, USA
Fax: (1) 914 271 58 56

STRASBOURG
Librairie Kléber
Palais de l'Europe
F-67075 STRASBOURG Cedex
Fax: (33) 88 52 91 21

Council of Europe Press/Les éditions du Conseil de l'Europe
Council of Europe/Conseil de l'Europe
F-67075 Strasbourg Cedex
Tel. (33) 88 41 25 81 - Fax (33) 88 41 27 80

02 388

What kind of legal measures should be taken to combat the illicit reception and distribution of encrypted television services? All European countries today have to answer this question in view of phenomena such as the installation of pirate relays or the piracy of decoding equipment, which entail important risks for the future of the audiovisual sector in Europe.

This recommendation is intended to offer guidance to member states on how to fight these new forms of piracy from a legal point of view. It highlights the activities of manufacture, importation, distribution, advertising, commercial promotion and possession, for commercial purposes, of decoding equipment as matters which should be considered unlawful. The recommendation also provides for a series of sanctions and remedies in the fields of penal, administrative and civil law which member states should envisage in their legislation for curtailing these practices.

Council of Europe Press

ISBN 92-871-2710-7