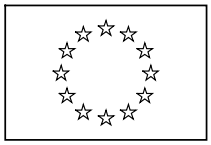


COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 24.04.2003
COM(2003) 198 final

ON THE LEGAL PROTECTION OF ELECTRONIC PAY SERVICES

Report from the Commission to the Council, the European Parliament and the European Economic and Social Committee

on the implementation of Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, and consisting of, conditional access

Executive Summary

This first report from the Commission on the implementation of Directive 98/84/EC, which aims to provide a minimum level of **legal protection within the EU of electronic pay services (**pay TV, radio and Internet services) **against piracy**, is part of the Commission's comprehensive Internal Market strategy to remove barriers to services. It describes and analyses the salient facts relating to the key provisions of the Directive, looks at how these provisions are implemented and enforced by Member States and Candidate Countries, and highlights current trends in piracy. It covers the period from adoption of the Directive in November 1998 through to the end of 2002.

The report finds that the knowledge-based economies of the 21st century are expected to rely increasingly on **pervasive electronic pay services** and that piracy will have the same detrimental effects in the knowledge society as white-collar crime and counterfeiting of goods in the 20th century. Legal protection against piracy of electronic pay services will make a major **contribution to achieving the Union's ambitious target of becoming the most dynamic and competitive economy by 2010**.

The report highlights the piracy resulting from the impossibility of accessing **protected satellite TV channels originating from other Member States**. It notes that EU citizens fail to understand why, within the internal market, they cannot obtain legitimate access to protected pay-TV services, even if they are prepared to pay. The report therefore calls upon the market parties to actively seek **contractual solutions** and states that the Commission will contribute to this process in its review of the Directive concerning copyright related to satellite broadcasting and cable retransmission.

The report shows that **implementation** of the Directive has not yet been fully achieved within the enlarged Union, that **enforcement** at national level has to be consolidated and that **joint efforts** are instrumental in fighting piracy effectively. Only if pirates do not find safe havens in Europe will it be possible to combat piracy. Therefore, the Commission will continue its co-operation with other European countries and relevant international organisations in an effort to create **a coherent pan-European legal framework against the piracy of electronic pay services**, in particular through rapid entry into force of Council of Europe Convention No 178.

The report observes that **pirating electronic pay services is considered to be a cyber crime**. It concludes that it would be **premature to propose amendments** to the Directive, but that the consultations and assessment undertaken in the context of the Report have enabled the Commission already to identify several issues which deserve further reflection in close co-operation with the Member States and industry. These issues include the need for a **balanced and coherent enforcement framework** applicable to all kinds of piracy and counterfeiting and agreed at Community level and the **distribution of keys and illicit devices** via the Internet.

TABLE OF CONTENTS

1. INTRODUCTION

This document contains the first report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the implementation of Directive 98/84/EC[1] on the legal protection of services based on, or consisting of, conditional access (referred to below as 'the Directive').

This Directive aims to provide a minimum level of legal protection within the EU of electronic pay services against piracy by prohibiting all commercial manufacturing, distribution and marketing activities related to pirate smart cards and other devices circumventing the access protection of pay TV, radio and Internet services.

Article 7 of the Directive provides that, not later than three years after the entry into force of the Directive,[2] and every two years thereafter, the Commission has to submit a report to the European Parliament, the Council and the Economic and Social Committee concerning the implementation of the Directive accompanied, where appropriate, by proposals, in particular as regards the definitions under Article 2, for adapting it in the light of technical and economic developments and of the consultations carried out by the Commission.

This report deals with the implementation of the Directive since its adoption in November 1998 through to the end of 2002.

The report describes and analyses the salient facts relating to the key provisions of the Directive and their implementation in national legislation. The report is based on the transposition information provided by Member States, the views expressed by market players, in particular on the development of piracy and enforcement by national authorities, and the Commission's own views and analysis. It also takes account of the results of an independent study commissioned in 1999 on the use of conditional access for reasons other than the protection of remuneration.

Furthermore, this report is part of the Commission's comprehensive Internal Market strategy to remove barriers to services.[3]

2. BACKGROUND AND CONTENT OF THE DIRECTIVE

2.1. Background

Technological progress, liberalisation and harmonisation of the legal framework resulted in rapid expansion of broadcasting channels and information society services in Europe during the last decade of the 20th century. These new services are mainly offered by commercial companies and financed either from advertising revenues and sponsoring or by the payment of fees and subscriptions. Typical examples of this

---

1 OJ L320, 28.11.1998, p. 54; see: http://europa.eu.int/comm/internal_market/en/media/condac/dir/index.htm

2 28.11.1998.

3 COM(2000) 888 final of 29.12.2000 "An Internal Market Strategy for Services"; see http://europa.eu.int/comm/internal_market/en/services/services/index.htm

development are satellite-based pay TV stations offering premium content channels (movies) or thematic channels on sports, lifestyle or travel.

In order to ensure that they are paid for their services, providers deploy so-called conditional access technologies, which make it impossible in principle to access the service in an intelligible form without the prior authorisation of the provider. While the service protected by conditional access may be widely receivable, it can only be viewed or listened to if the viewer/listener uses a special decoder, often together with a smart card[4] bought from the service provider. This method is highly effective in terms of ensuring payment, provided that only those members of the public who have paid for the device and whom the provider therefore seeks to reach are capable of decoding the service.

Today, there are about 126 TV channels transmitted by satellite. Half of these channels are encrypted by 12 different conditional access systems.

Satellite	Platform	Conditional Access System	Main Market
Astra	BSkyB	Videoguard	United Kingdom, Ireland
Astra	Canal Satélite Digital	Mediaguard	Spain
Astra	CanalSatellite	Mediaguard; Viaccess	France
Astra	CanalDigitaal	Irdeto; Mediaguard	The Netherlands
Astra	Première World	Betacrypt	Germany, Austria
Astra	Wizja TV	Cryptoworks	Poland
Astra	UPC Direct	Cryptoworks	Hungary
Astra	UPC Direct	Cryptoworks	Czech Republic; Slovakia
Eutelsat	Tele+ Digitale	Mediaguard; Videoguard	Italy
Eutelsat	Absat	Viaccess	France, Belgium, Luxembourg
Eutelsat	TPS	Mediaguard; Viaccess	France
Eutelsat	Stream	Mediaguard; Videoguard	Italy
Eutelsat	Alpha Digital	Nagravision	Greece; Cyprus
Eutelsat	Nova	Irdeto	Greece; Cyprus
Eutelsat	Cyfra+	Mediaguard	Poland
Eutelsat	Polsat	Nagravision	Poland
Hispasat	TV Cabo	Nagravision	Portugal
Hispasat	Via Digital	Nagravision	Spain
Sirius	Viasat	Viaccess	Scandinavia
Thor	Canal Digital	Conax	Scandinavia

Table 1: Main satellite pay TV providers in Europe (2002)

Conditional access is a set of technologies which can be used, and in practice are used, for several different purposes. In addition to remuneration of the service itself, conditional access is also used, often in parallel, to restrict the potential audience to a particular territory, for example, for copyright reasons, or to a particular class of users, for example, by excluding minors.

The advent of pay television has also heralded the start of a flourishing commercial piracy industry. Illicit access to a service protected by conditional access has several adverse effects on the service provider concerned. By depriving providers of remuneration, piracy poses a direct threat to the economic viability of the service

[4] Smart cards or "chip cards" are plastic cards of the size of a bank card, embedded with a microprocessor and memory, which are able to process data. Basically, smart cards are small, portable and often secure computers.

providers concerned, to the competition between them and, hence, to the diversity of services offered to the public.

Technology alone cannot provide the full answer to the piracy problem.[5] In order to combat piracy, some Member States have introduced new legislation, in parallel with the technical countermeasures put in place by service providers. Others have tried to apply existing provisions of criminal law, unfair competition law or tort law. Some Member States had no legal protection at all. A Commission survey during 1995[6] showed substantial differences in legal protection between the Member States in terms of scope, prohibitions and sanctions. After a wide-ranging consultation process the Commission proposed harmonising the legal protection of all electronically provided services using any form of conditional access to ensure the remuneration of the service. At the end 1998 Directive 98/84/EC[7] was adopted.

2.2. Key provisions of the Directive

The Directive aims to combat piracy against "protected services" by prohibiting commercial activities related to "illicit devices". This legal protection is based on the concept of curbing the illegal "upstream" commercial decoder market, i.e. preventing illegal decoders and related devices from becoming available to end-users. This approach works well if the specialised technology and knowledge to manufacture illegal decoders and smart cards are not available to interested end-users.

The Directive also consolidates the functioning of the internal market by denying Member States the possibility of restricting the free movement of conditional access devices or the free circulation of pay services for reasons related to the infringing piracy activities specified by the Directive.

2.2.1. Definitions

Protected service

The Directive covers not only conventional television and radio broadcasting services, but also all kinds of interactive online services (information society services)[8]. Services have to be understood within the meaning of Article 50 of the Treaty (ex Article 60),[9] as interpreted by the Court of Justice.[10] The Directive

---

5 Back in 1991 the Council of Europe already concluded that it was necessary to complement technical protection by appropriate legal measures; see Recommendation R(91)14 of the Committee of Ministers on the legal protection of encrypted television services; http://cm.coe.int/ta/rec/1991/91r14.htm

6 COM(96)76 final of 06.03.1996 – Green Paper on the legal protection of encrypted services in the internal market; see http://europa.eu.int/comm/internal_market/en/media/condac/dir/legproc_en.htm

7 Directive 98/84/EC only ensures the legal protection of conditional access services. The provision itself of these services as well as the technical requirements for legitimate conditional access devices are covered by other Community Directives, e.g. Directive 2002/19/EC (Access Directive) and 2002/22/EC (Universal Service Directive); OJ L108, 24.04.2002; http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm

8 Information society services are defined in Article 1(2) of Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations; OJ L217 of 05.08.1998, p. 18.

9 Services shall be considered to be "services" within the meaning of this Treaty where they are normally provided for remuneration, insofar as they are not governed by the provisions relating to the freedom of movement for goods, capital and persons.

protects "content" services irrespective of the technical characteristics of the transmission method used. The Directive is the first Community Directive to apply to both broadcasting and interactive services. It can be considered as the first occurrence of "legal convergence"[11] in Community legislation.

However, in order to benefit from the protection provided for in the Directive, the services need to use some form of conditional access for the purpose of obtaining remuneration for the service provider concerned. Remuneration can be in the form of a subscription (for example, for viewing the complete offer of a particular channel during an agreed period) or the payment of a fee (for example, for viewing one particular movie). These payments directly to the service provider seek to ensure the economic viability of the service.[12] Business models whereby a particular service is provided against payment by the recipient, but whereby ancillary services are provided as well without direct payment but with conditional access protection, are also covered (for example, "bonus tracks" to be downloaded from the Internet for legitimate owners of the original audio CD). Without such a link between remuneration and a conditional access protected service, no legal protection can be granted under the Directive.

The provision of conditional access to radio, TV and information society services, referred to in the Directive as a service in its own right, is also covered by the concept of "protected service". While the provider of such a service does not have a direct economic interest in the "content" services its conditional access is protecting, it has an immediate economic interest in protecting the security offered by its conditional access technology. Successful piracy against its protection technology directly undermines the confidence of its clients in the protection capabilities of the service concerned and, consequently, its economic viability.

Conditional access

The Directive is formulated in a technology-neutral way. By not making reference to a particular technology, but by using high-level functional definitions, the Directive becomes more "future-proof" and less "maintenance prone", as well as providing a more stable legal framework and therefore optimal legal security.

Not only typical conditional access technologies based on cryptography, such as used in pay TV, are covered, but also any other technology denying access to the service without the prior approval of the service provider, such as user-ID/password schemes often used by pay services provided over the Internet.

---

10 In accordance with the case law of the Court of Justice the concept of a service "normally provided for remuneration" does not make reference to specific means of financing. "Article 60 (now Article 50 EC) does not require the service to be paid for by those for whom it is performed – Case C-352/85 Bond van Adverteerders [1988] ECR 2085 §16 – but to the existence of a consideration for the service in question – Case C-109/92 Wirth [1993] ECR I-6447 §15.

11 Communications and information technologies are progressively using the same, or at least similar, types of (digital) technology. This "technological convergence" increasingly affects markets and service provision in the field of broadcasting, interactive services and electronic communications, and consequently the related regulation. In such an environment where boundaries tend to blur, "legal convergence" by means of merging legal instruments on the basis of a common technology-neutral approach is often considered the best regulatory response.

12 See Recital 6 of the Directive.

Illicit devices

Illicit devices have to be designed or adapted to give intelligible access to a protected service without the authorisation of the service provider. Typical examples of illicit devices are special purpose hardware devices or software programmes built to bypass the conditional access protection. Due to developments in smart card-related technologies, fully functional smart cards in the form of modified original cards, or duplicates of original cards, or specially produced completely new pirate cards are currently the most often used illicit devices. However, blank smart cards or standard smart card programmers[13] do not as such qualify as illicit devices.

2.2.2. Infringing activities

Contrary to other parts of the Directive, the provisions on infringing activities are very prescriptive. A detailed catalogue of activities to be prohibited covers the full business chain of activities from the initial production to the after-sales maintenance and repair of illicit devices, including all forms of commercial communications.[14]

The Directive imposes sanctions only on commercial activities[15] favouring unauthorised reception, not on unauthorised reception as such. It clearly reflects the approach to stop piracy "upstream", i.e. activities enabling illegal access.

2.2.3. Sanctions and remedies

The Directive does not oblige Member States to impose specific sanctions, but limits itself to stipulating that sanctions have to be effective, dissuasive and proportionate.[16] The Directive neither fixes the level or the type[17] of the penalties, and nor does it prejudice the application of certain provisions of national criminal law.[18]

Member States have to make a set of appropriate remedies available to providers of "protected services", including, as a minimum, an action for damages, an injunction or other preventive measure as well as the possibility, where appropriate, of disposing of illicit devices outside commercial channels.

---

13 A smart card programmer is a hardware device connected to and controlled by a PC capable of loading data into the memory of the smart card.

14 Recital 14 explains what has to be understood by this concept, which, at the time of adoption of the Directive, did not yet exist in Community law.

15 Recital 13 of the Directive clarifies the concept of "for commercial purposes" by making explicit reference to "direct and indirect financial gain".

16 This approach is commonly used in internal market-related legislation. It is enshrined in the Commission Communication on the role of penalties in implementing Community legislation – COM(95) 162 and was applied for the first time by the Court of Justice in its judgment in Case 68/88, Commission vs. Greece [1989] ECR-2965.

17 Recital 23 clarifies that Member States are not obliged to impose criminal sanctions.

18 Recital 22 allows, for example, a "knowledge test" for infringing activities. Recital 23 allows, for example, the seizure of illicit devices.

2.3. Questions raised during the adoption of the Directive

2.3.1. Use of conditional access for other reasons than the remuneration of the service provider

Conditional access technologies control and secure access to electronically transmitted "content" services. These technologies allow their users to determine the precise conditions under which access is granted.

The Directive exclusively protects service providers using conditional access for the purposes of ensuring that they are paid. However, conditional access may, and in practice does, serve many other purposes. Most conditional access systems used by satellite pay TV operators not only ensure payment but also aim to restrict the potential audience of the broadcast to a particular territory (often a Member State), mostly for copyright reasons. Conditional access is also used to protect minors against offensive adult content.

During the adoption process of the Directive there was broad discussion on the need and wisdom of extending the scope of the legal protection offered by the Directive to the use of conditional access for copyright reasons. Such an extension would entitle copyright holders, in parallel with and independent of the providers of protected services, to bring an action against and seek compensation for damages from illicit device manufacturers and merchants.

Eventually, it was decided not to bring copyright protection under the umbrella of the Directive. One of the main reasons was that as Community law stood at that point in time producing and selling illicit devices could not be qualified as an infringement of copyright.[19] Another reason was to be found in the ongoing negotiation of a draft Directive on copyright in the Information Society, which contained provisions on technical protection measures and anti-circumvention and was considered complementary to the Conditional Access Directive.[20]

The Commission agreed to call for a study to examine the legal and economic implications of the use of conditional access for reasons other than the protection of remuneration.[21] The study, which was finalised in April 2000, focused on those "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 identified a variety of such interests, ranging from compliance with contractual and statutory obligations to marketing and advertising strategies, security aspects, and indirect remuneration. In all cases the study found that the decision to use conditional access was based on valid economic and legal considerations. Some of these interests were more often found with broadcasters, others more often with information society service providers. It shows that conditional access is often used

---

19 Recital 21 of the Directive clarifies that the Conditional Access Directive is without prejudice to the application of Community rules concerning intellectual property rights.

20 See COM(97) 628 final of 10.12.1997, p. 33.

21 This study was awarded to the Institute for Information Law (IVIR) of the University of Amsterdam. The final report, dated April 2000, is available at http://www.ivir.nl/publications/other/ca-report.htm or at http://europa.eu.int/comm/internal_market/en/media/condac/backgrnd/index.htm

for more than one reason at the same time. Apparently, the requirements from the content industry (copyright) and the use of wide-area transmission techniques (satellite) are the main driving forces behind the use of conditional access for non-remuneration reasons.

The study forecasts that the use of conditional access for non-remuneration reasons will grow, but that it is still too early to predict seriously and reliably how the market will develop and what the impact of the increased use of conditional access will be. The study indicates that the risk of exposure to piracy will be similar for both remunerated and non-remunerated cases.

2.3.2. Commercial versus private purposes

The list of infringing activities set out in the Directive is mainly based on the list of unlawful activities laid down in Recommendation R(91)14 of the Council of Europe.[22] This Directive and the Recommendation as its conceptual predecessor consider that the most effective way of thwarting piracy is to concentrate on commercial activities enabling illegal access.

However, at the time of the negotiation of the Directive a few Member States had made certain private acts, such as private possession of an illicit device and/or unauthorised private reception itself, punishable. During the negotiation of the Directive different views existed among the Member States and the Community Institutions as to the need and wisdom of extending the harmonisation of infringing activities beyond commercial activities. In the end it was agreed that the Directive would only cover commercial activities, but that it was possible for Member States to prohibit the private possession of illicit devices under national law.[23]

Similar discussions also took place during the adoption process of the Copyright in the Information Society Directive, resulting in a more or less comparable solution.[24]

3. IMPLEMENTATION OF THE DIRECTIVE

3.1. Notification of implementation measures

The Directive granted Member States a period of one and a half years to implement its provisions. By the deadline for transposition, i.e. 28 May 2000, only very few Member States had notified implementation legislation to the Commission.

In accordance with the procedure laid down in Article 226 of the Treaty (ex Article 169) for non-notification of national implementing measures, letters of formal notice were sent out to the Member States that had failed to do so. Following these letters, a large majority of Member States duly notified their implementing measures.

---

22 For more information see Chapter 6 of this Report.

23 See Recital 21 of the Directive.

24 For more details see Directive 2001/29/EC, Articles 6.1, 6.2 and 6.3, and Recital 49; OJ L167 of 22.06.2001, p. 10.

As at the date of this Communication the Commission has been obliged to refer several Member States (Greece and Spain) to the European Court of Justice for failure to notify.[25]

Several notifications do not include all the information needed for the Commission to assess the completeness of national implementation and its compatibility with Community law. In order to clarify this situation, bilateral discussions are currently taking place between the Commission and the Member States concerned. If necessary, the Commission will commence infringement proceedings under Article 226 against those Member States which, in the view of the Commission, do not implement the Directive with the required specificity, precision and clarity.[26]

3.2. Current state of implementation by Member States

Quite a long period of time elapsed between the entry into force of the Directive and the promulgation of national legislation implementing it. Most of the legislation entered into force from the second half of the year 2000 onwards.

Year	Member State
<1998	France – The Netherlands
1999	
2000	Austria – Ireland – Italy – Sweden – United Kingdom
2001	Denmark – Finland – Portugal
2002	Germany – Luxembourg – Greece
future	Belgium– Spain

Table 2: Year of entry into force

A continuously updated overview of the implementation of the Directive by the EU and EEA Member States and the Candidate Countries, including extensive references to national law accompanied by informal translations into English, is available on the EUROPA website.[27]

As was to be expected, Member States have implemented the Directive in many different ways in their national legislation. Some have chosen to cover conventional radio and TV services in media legislation and information society services and conditional access services in their own right in cybercrime or related legislation. Other Member States have preferred a single (set of) provision(s) covering all services in either the criminal code or a special law.

By and large, the national implementing measures notified to the Commission meet the requirements of the Directive. In the majority of Member States all protected services are adequately covered, although it is unclear in a few Member States whether conditional access services in their own right are indeed protected. Some minor points of clarification are still being discussed between the Commission and the Member State concerned.

---

25 Spain: Case C-58/02; Greece: Case C-219/02; Commission Press Release IP/02/455 of 22.03.2002; http://europa.eu.int/comm/internal_market/en/media/infr/02-455.htm

26 Case C-197/96, paragraphs 14 and 15.

27 http://europa.eu.int/comm/internal_market/en/media/condac/natimp/index.htm

A similar situation exists with regard to the set of infringing activities to be prohibited pursuant to Article 4 of the Directive. In a few cases a particular infringing activity is not explicitly prohibited, because it is presumed to be covered by a more generic term or by an existing general clause of the national criminal law. In order to ensure legal certainty for citizens and business the Commission is discussing these cases with the Member State concerned.

While the Directive does not oblige Member States to impose criminal sanctions,[28] all Member States but two (Italy and Portugal) do impose sanctions for what they consider the main infringing activities (manufacture and sale), with imprisonment and/or fines. Obviously, some divergence exists in how the individual Member States interpret the infringing nature of the prohibited activities and the necessary deterrence.

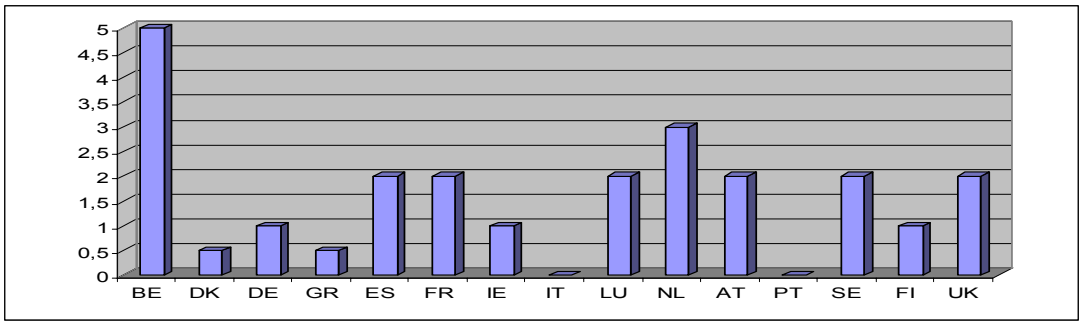


Chart 1:Maximum term of imprisonment in years for the main infringing activities

A few Member States have introduced a system of modulated sanctions. By integrating prohibitions and sanctions into criminal law, the classical range of secondary criminal offences (complicity, instigation, aiding and abetting) and criminal procedures (search and seizure, forfeiture) are also available.

In a few Member States (Austria, Germany and Italy), where existing legal provisions could already be used to prosecute certain forms of piracy, the introduction of specific, but less severe sanctions for the infringing activities defined by the Directive has resulted in a *de facto* reduction of legal protection in those Member States.[29]

In most Member States appropriate remedies are available to injured service providers. In the few cases where it is not completely clear whether all remedies required by the Directive have been made available, the Commission is seeking clarification from the Member State concerned.

The Commission concludes that implementation of the Directive in national legislation does not yet appear to have been fully achieved by all Member States. Two Member States still have to complete their national implementation process, while there is some uncertainty in several others as to their completeness and compatibility. The Commission will continue to examine the national measures in question and vigorously pursue its efforts to have the Directive fully implemented.

---

28 Recital 23, second sentence, of the Directive.

29 Lex specialis derogat generali.

3.3. National provisions beyond the requirements of the Directive

The Directive introduces only a minimum level of legal protection against piracy and grants Member States a lot of flexibility and discretion in tailoring their national anti-piracy regime to their own needs and policies. Several Member States have used this prerogative and extended the definition of protected services as well as infringing activities, sanctions and remedies.

A substantial number of Member States neither explicitly require the use of conditional access nor focus only on remuneration of the service provider, but grant protection of all services against unauthorised access or access without permission.

Similarly, a minority of Member States prohibits personal use and/or private possession of illicit devices.

Some Member States have made explicit provision for specific sanctions (publication of judgements, forfeiture of profits) and remedies (compensation of lost profits, transfer of profits made).

In a few Member States a National Supervisory Authority (sometimes the telecommunications authority, sometimes a special service) has been charged with the monitoring and surveillance of the market and (partial) enforcement of the law.

3.4. Enlargement

The Candidate Countries have to implement the Directive as part of the *acquis communautaire*. Timely implementation accompanied by effective enforcement is of vital importance in the fight against piracy within the Union as well as within prospective member states. In parallel with enhancing protection in the EU, acts of piracy related to pay TV and Internet services are tending increasingly to shift towards central Europe.

Enlargement is one of the Commission's top priorities in 2002[30] and 2003.[31] The Commission is actively monitoring implementation and assists as much as possible the Candidate Countries with the drafting and subsequent practical implementation of the relevant national legislation transposing the Directive.

While much effort is still required, progress so far has been encouraging. Four countries have already put the major part of the necessary legislation in place. Several other Candidate Countries are currently preparing their draft implementing legislation and envisage final adoption by the end of 2003. The remaining countries have confirmed that they intend to adopt the necessary measures by the date of accession in 2004 at the latest.

As already emphasised in the previous chapter of this report, application of the legislation in force is the primary duty of the national authorities. In order to be ready to apply the legislation once it has entered into force, the enforcement authorities of the Candidate Countries have to be trained.

---

30 COM(2001) 620 final of 05.12.2001, p. 14.

31 see Press Release IP/02/338 (Annual Policy Strategy for 2003).

Candidate Countries are showing encouraging progress with the implementation of the Directive, although much effort still has to be made.

The Commission will continue to work together with all Candidate Countries towards an adequate level of administrative and judicial capacity by the time of accession.[32] With the help of specialised industry players, special training seminars for the police and judicial authorities can be planned.[33]

4. MARKET DEVELOPMENTS AND APPLICATION OF THE DIRECTIVE

4.1. Consultation of the market parties

In preparation of this report the Commission consulted the main industry stakeholders affected by the piracy of conditional access protected services and the related legal countermeasures. In line with the commitment taken in its White Paper on European Governance[34] and its recent proposals on better lawmaking,[35] the Commission undertook this consultation in order to encourage an open dialogue on the piracy problems encountered on the market and to help collect and analyse new and existing information in the technically and legally advanced field covered by the Directive. The Commission did not undertake a full-blown impact assessment[36] because the Directive was still being transposed into national legislation during the reporting period.

The results of the consultation provided significant input into the preparation of this report and its possible follow-up.[37] Obviously, market players are very reluctant to discuss the details of piracy and how it affects their business. Too much openness might prove to be counterproductive due to the potential impact on the confidence of customers in the quality of the protection offered, the competitive position on the market and shareholder value. Industry associations like AEPOC,[38] STOP[39] or the ICRT[40] have proven to be very instrumental in conveying the concerns and illustrating the problems met by the members they represent. Whilst understandable, this protective attitude complicates efforts to get a clear picture of the size and impact of the problem as well as identifying effective and efficient solutions.

---

32 COM(2002) 256 final of 05.06.2002.

33 See also chapter 4.3 on enforcement.

34 COM(2001) 428 final of 25.07.2001; http://europa.eu.int/comm/governance/index_en.htm

35 COM(2002) 275 final and COM(2002) 277 final of 05.06.2002.

36 COM(2002) 276 final of 05.06.2002.

37 The Commission has received written submissions from AEPOC, EBU, AER, ACT, MPA, ACTI, ACCeS, DVD, STOP Sweden, STOP Denmark, STOP Norway, ICRT and the KirchGruppe. In addition more informal, bilateral meetings were held with several market players.

38 AEPOC, the European Association for the Protection of Encrypted Works and Services, represents Betaresearch, BskyB, Canal+, Canal+Polska, Canal+ technologies, Conax, Eutelsat, IrdetoAccess, Motorola, NDS, NTV-Plus, Pace, Philips Digital Networks, Première, Rai, SCM Microsystems, Société Européenne des Satellites, Sogecable, Stream, Tele+, Thompson, TPS, UPC and Viaccess-France Telecom; see http://www.aepoc.org/

39 STOP, the Scandinavian TV Organisations against Piracy, exists in Finland, Sweden, Norway and Denmark (http://www.stop.dk)

40 ICRT, the International Communications Round Table, represents American Express, AOL Time Warner, Springer, Bertelsmann, British Telecom, Coface, EDS, IBM, Kirch, Philips, KPN, Lagardère, Microsoft, NCR, News Int, NewsCorp, Reed-Elsevier, Reuters, Siemens, Sony, Walt Disney, UPC, von Holtzbrinck, Vivendi, VNU, Yahoo (www.icrt.org)

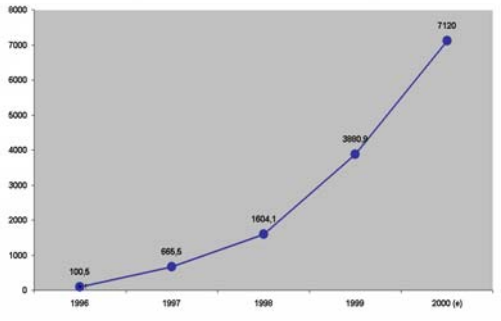
In return, and in line with its efforts to communicate more actively with the general public on European issues, the Commission has completely refurbished its web pages on EUROPA relating to the Directive and its implementation.[41]

4.2. Combating pir@cy – a moving target

Audio-visual piracy and particularly piracy related to pay services is developing along the same lines as the services it tries to exploit. Initially, it was possible to hack encrypted analogue pay TV channels by means of modified decoders. This kind of piracy required specialised knowledge of analogue TV technology and electronics as well as special manufacturing skills.

Services targeted by pirates

Digitalisation led to an enormous upsurge in distribution channels and supply of content, resulting *inter alia* in a fast developing digital pay TV market. Subscription revenues have grown exponentially since 1996. Recent Commission studies indicate that subscriptions are gradually gaining in importance. Digital TV subscription revenues grew from less than 25% of industry revenues in 1995 to approximately 35% in 2000.



Source: IDATE and 7th Implementation Report Telecom

Chart 2: digital TV subscription revenues since 1996 (in M€)

With the migration to digital of analogue cable networks and terrestrial television, digital pay TV services are progressively being provided via these new distribution channels (for details see Table 3). Recent statistics more or less confirm this trend and indicate that by 2008 digital TV will be present in 73% of European homes (122 million households).[42]

The proliferation of digital TV will result in wide deployment of digital decoders, either in hardware form (set-top boxes and intelligent TV sets) or in software form (specialised software on a PC with a DVB card[43]).

The downside of this technical convergence is that current digital satellite TV piracy will spread into new areas like digital terrestrial television and digital cable television and become increasingly more widespread.

---

41 http://europa.eu.int/comm/internal_market/en/media/condac/index.htm

42 Strategy Analytics, 28 May 2002; http://www.strategyanalytics.com/press/prsk012.htm

43 A DVB card is computer hardware designed for receiving, decoding and displaying digital television conforming to the European DVB standards on a standard Personal Computer.

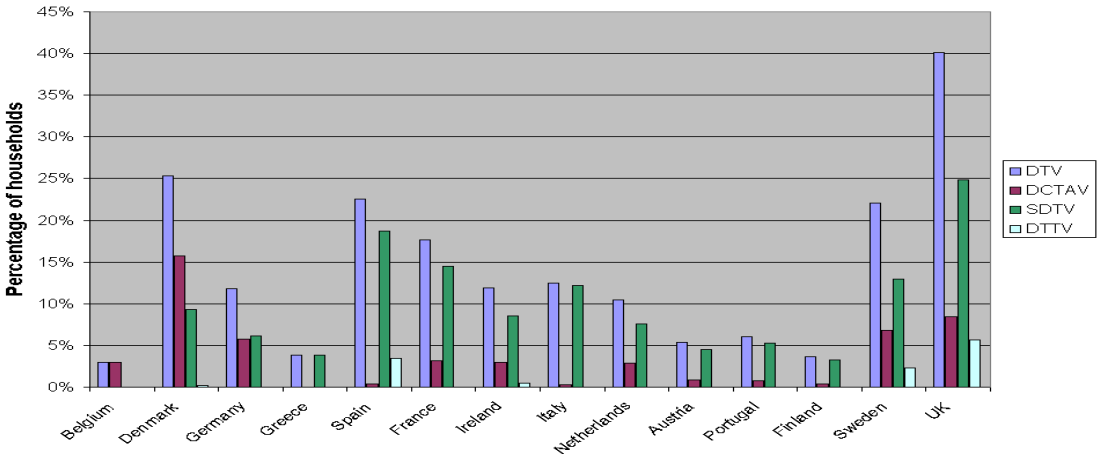
Digital TV households	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
Satellite											
Digital Satellite TV Households (M)	0.0	0.4	1.9	4.1	8.3	14.3	19.2	24.0	28.2	32.3	35.9
Cable											
Digital Cable TV Households (M)	0.0	0.0	0.1	0.8	1.7	3.2	6.1	10.7	16.3	22.5	28.8
Terrestrial											
Digital Terrestrial TV Households (M)	0.0	0.0	0.0	0.0	0.5	1.3	2.1	3.5	5.1	7.1	8.8
TOTAL DIGITAL TV HOUSEHOLDS (M)	0.0	0.4	2.0	5.0	10.5	18.7	27.4	37.8	48.7	60.1	70.8

Source: Strategy Analytics, Feb 2001 and 7th Implementation Report Telecom

Table 3: Digital TV households in the EU (plus Norway and Switzerland), trend and forecast

National digital television markets are at very different stages of development in the Member States. Differences in penetration between the different digital TV delivery mechanisms will influence the level of piracy in each Member State (for details see Chart 3).

Unlike pay TV, pay radio services have so far not been widely deployed in Europe. Radio in Europe is mainly based on free-to-air business models.[44] A few pay radio stations are operational in the USA, but only on the basis of proprietary receiver and conditional access technology. These stations promote their pay services by stressing the high audio quality, coast-to-coast coverage and the large variety in commercial-free music, sports and news programming. Nothing similar has yet been experienced in Europe, although through digital radio pay radio services are expected in the future, for example, in combination with other technologies like mobile telephony.



Source: prepared by EC services from Strategy Analytics data

DTV: Digital TV
DCATV: DTV by cable
SDTV: DTV by satellite
DTTV: Digital Terrestrial TV

Chart 3: Digital TV EU household penetration in 2001, by Member State and delivery mechanism (percentage of households)

With the downturn in the Internet economy and the weak advertising market, providers of information society services are launching premium services for a fee in order to generate alternative revenue sources and to create lasting relationships with their customers supporting their digital lifestyle. These subscription-based Internet services are mainly protected by username/password mechanisms and vary from

44 Occasionally, thematic radio channels are only made available to subscribers of premium packages; for an example see http://www4.telepiu.it/v4_intrattenimento/multimusica/multimusica.asp

online games, advanced document searches, full editorial offerings of online newspapers and specialised journals to music downloads and on-demand movies. A flourishing category of pay services are the online update services available to the owners of the original software programs, whereby the serial number of the original CD acts as access authorisation. Market players and legislators are currently watching with great interest and expectation these first and probably still immature attempts to generate income from online content offerings.

Piracy methods and tools

Most of today's piracy of digital pay TV takes place at the level of the smart card or the decoder software. An exquisite range of websites and message boards provide in-depth background information on the different conditional access systems, tutorials on how to (re-)program smart cards as well as references to where to "find" essential key material. Smart card technology has entered the main stream of business applications. The hardware and software tools to program these cards are widely available, because smart cards and their programmers are also used for legitimate purposes. It is obvious that user-friendliness of the necessary tools and the availability of knowledge and information via the Internet have facilitated piracy of digital systems considerably.

Pirate smart cards are often based on the original smart cards issued by pay-TV operators. Disabled cards, or cards only giving access to the basic service offering, are modified (so-called MOSCs[45]) and turned into cards giving full access to the whole package of services. Digital pirate smart cards, often called DPSCs, are either functionally identical "clones" of original cards or newly programmed smart cards.

Professional pirates are well-equipped and produce large quantities of MOSCs and DPSCs. The quasi-industrial production and distribution of these pirate cards requires highly "professional" business-type working methods, often involving organised crime.

Less industrial, but nevertheless no less damaging, is the "local' production on a much smaller scale of pirate cards on the basis of publicly available empty smart cards. This kind of pirating uses "do-it-yourself" hardware and information mainly available via the Internet. Profits are made from selling blank cards and programmers or complete satellite reception installations, including a counterfeit access card[46] at attractive prices. These pirates are also used by organised crime as a distribution channel for the pirate cards produced by professional pirates. Often the commercial nature of this form of piracy is difficult to establish because calculating perpetrators reduce their "penal" exposure to the maximum.

Private individuals also take part in this "cottage-industry" form of piracy. As "casual pirates" they use the same hardware and information and are offering "self-made" cards as a small service to friends, neighbours or colleagues at work, often in exchange for cash or other valuables like pirate copies of software, music CDs or DVDs.

---

45 Modified Original Smart Card.

46 The marginal costs to produce such a card are insignificant (less than 1%) in comparison to the real cost of the subscription.

Increasingly, technically savvy viewers themselves are producing pirate cards for their own private use. All they need to do is to acquire the necessary know-how from hacker sites and to make a one-time modest investment in the basic hardware.

Two relatively new and extremely dangerous forms of piracy are developing very quickly at present. The first is based on the use of ordinary PCs equipped with DVB TV cards and software decoders. These powerful software decoders, which emulate the conditional access hardware module and the smart card, are distributed over the Internet. The second form centres on the possibility of modifying commercially available common interface conditional access modules (CAMs) by applying specialised software "patches", with the result that a valid smart card is no longer necessary (so-called FreeCams). Both forms rely on ultra user friendly distribution over the Internet, which make them the potential piracy killer application.

All pirates, except maybe the most professional ones, depend for the availability of keys, circumvention tools and instructions, etc., on private hacker websites. These websites are the essential link in the piracy business chain because they are the source of the necessary material. Therefore, they are also the Achilles heel of a major part of the piracy business. Many of these hacker sites present themselves as private initiatives without any economic backing from commercial partners. While this may be true for some of them, others use banner advertising or recommend particular product brands, suggesting some form of commercial relationship. Websites need hosting computers and Internet connections, which are never for free.

Damage caused by piracy

Audio-visual piracy is not a "victimless" crime. Most pay-TV broadcasters operate within narrow financial margins. The difference between commercial success and bankruptcy is usually very small in emerging industries of this kind and often depends on a progressively expanding paying audience and ARPU.[47] The number of pirate viewers watching without payment can make the difference.

Piracy does not only deprive operators of their revenues, it also increases the operating costs as well as the need for additional investment. Industry sources claim that the replacement of one smart card in a major card swap-out costs about €11.[48] One major pay-TV operator claimed to have spent over €35 million to develop its widely used set-top box middleware and conditional access system.[49]

Piracy also has a negative impact on the revenues of the national treasury. Pirates do not pay taxes on their services; and legitimate providers pay less VAT and company taxes due to lower turnover and lesser profits.

Law-abiding consumers can easily be misled about the origin of decoders and smart cards. They are the first to bear the consequences of the fraudulent behaviour of pirates when the operator disables their pirate smart card or takes other countermeasures.

---

47 Average Revenue Per User.

48 New Media Markets – 31.05.2002, p. 6.

49 New Media Markets – 15.03.2002, p. 5.

Indirectly, piracy also distorts other audio-visual markets. It not only affects the retail market of set-top boxes and subscriptions, it also has a potentially detrimental effect on the cinema sector and the rental of video cassettes and DVDs due to the availability of premium material via illegal access to electronic pay services.

Information provided by AEPOC,[50] the European Association for the Protection of Encrypted Works and Services, showed that lost revenue from piracy in Europe exceeded €200 million in 1996. AEPOC estimates that, due to the increased annual legal turnover of pay-TV operators, the illegal turnover connected to piracy is in the order of €1 billion yearly. Recently, ITV Digital estimated its lost revenues from smart card piracy to be over £100 million.[51]

Apart from the economic damage it produces, the act of piracy itself also causes "societal" damage. Burglary and theft are per definition unacceptable in any civilised society because they attack the heart of our system of values. The cyber equivalents of these offences and the damage done to the public interest should be seen in the same light.

Countermeasures

Pay-TV operators have a long tradition of fighting off piracy. In the early days of pay TV, operators avoided legal actions in order not to make the general public aware of the vulnerability of their services. Therefore, traditionally the first answer to piracy is technical countermeasures. Today, operators exploit all countermeasure capabilities of their current operational system, including key updates and blocking of known pirate smart cards.

Operators are also continuously and routinely monitoring the piracy market and analysing new pirate devices and methods in order to keep abreast of piracy and to strike back with counterattacks. They reduce the vulnerability of their systems by upgrading the encryption and enhancing the key schemes used to identify (individual) users. Recently, several major operators have started replacing all legitimate smart cards with more secure ones. This swap-out of millions of cards is a major logistic challenge for these operators, the cost of which illustrates their determination to combat piracy.

There are, however, practical limits to these efforts due to the costs involved, the inconvenience for legitimate viewers and the technical possibilities of the system concerned. At that point effective enforcement of legal protection becomes the next line of defence.

4.3. Enforcement

Most Member States have only recently brought their national legislation into line with the Directive. Therefore, it is still rather early to get a complete and comprehensive picture of the practical effects of this new legislation on piracy and the fight against it. National enforcement authorities as well as the industry players concerned have to become accustomed to the new legal framework and how to make the most of its possibilities.

---

50 http://www.aepoc.org/

51 New Media Markets – 15.03.2002, p. 5.

Several market players responding to the Commission's consultations expressed their concern with the patchy implementation of the Directive and the reluctant attitude of the national enforcement authorities to investigate and prosecute suspected perpetrators. They draw attention to the fact that audio-visual piracy is a technically and legally complicated offence and highlight the need and their readiness to co-operate, assist and where necessary educate national authorities on the basis of joint efforts. Several examples of successful partnerships against pirates have shown that such an approach can work and should encourage authorities and service providers not yet participating to embrace this mutually beneficial approach. Practical co-operation should be obtained through training seminars, the creation of dynamic webs of persons and authorities involved in the fight against this kind of piracy, plus exchanges of best practices and information throughout the enlarged Union[52].

Most respondents emphasise the radical changes in piracy due to the Internet and their concern that the current legal framework was not designed with this kind of threat in mind. The commercial nature of hacker sites is often difficult to establish. The necessary key material is readily available on the Internet, allowing individuals to render pirate services to friends, most of the time without any commercial purpose. They complain that blank cards and programmers qualify as illicit devices only in very specific circumstances. Calculating perpetrators are aware of the deficiencies of the law and adapt their working methods in order to remain outside illegality as long as possible.

Sometimes some authorities seem to be inclined to refrain from enforcement on the basis of penal law and urge service providers to defend themselves in first instance by seeking civil remedies through court actions. While in certain cases acceptable, such a policy does not encourage service providers to publicly report piracy cases and may deny them the protection offered by criminal law. It makes them vulnerable to counterclaims for damages and negative publicity. Reluctance on both sides results in a lack of reliable data on the intensity and type of piracy, which further complicates policy-making and enforcement.

All market players ask for at least the private possession and personal use of illicit devices to be included in the definition of infringing activity. In the Nordic countries this approach seems to have been quite successful in repressing piracy.

While recognising the difference in scope of protection, quite a few respondents highlighted the similarity between enforcement measures, the procedures to be followed and the national enforcement authorities relating to conditional access piracy, on the one hand, and the measures relating to counterfeiting and copyright piracy, on the other.

---

[52] A typical example of this kind of joint effort is the e-S.PA.C.E. Dublin 2001 project, implemented under the EU Falcone programme, under which the Irish Garda National Bureau of Criminal Investigation and Microsoft teamed together and produced a training CD on software piracy and counterfeiting.

The Commission urges Member States and Candidate Countries to step up enforcement and to give providers of pay services adequate protection against pirates enriching themselves at their expense.

The Commission will continue to consult Member States and Candidate Countries on any remaining enforcement difficulties in an attempt to identify and combat loopholes in the legislation.

Industry and enforcement authorities should continue to develop joint efforts to curb piracy.

The Commission will continue supporting these developments as much as possible both from its funding programmes, including the AGIS Framework Programme on police and judicial co-operation in criminal matters[53] and from the resources available for assisting Candidate Countries to boost their administrative and judicial capacity.

4.4. Piracy-prone business practices

The Commission's attention is regularly drawn to the fact that citizens are not allowed to access protected satellite TV broadcasts originating from a Member State other than the one in which they are residing and readily accessible at moderate cost via satellite dishes,[54] despite the fact that they are willing to pay for such access. Service providers often argue that they do not hold the rights for the country of residence and that they are obliged to use conditional access technologies as a means of limiting access and protecting copyright. Citizens fail to understand that within the internal market they cannot obtain legitimate access to protected pay-TV services, even when they are prepared to pay the subscription fees and the handling costs.

It is obvious that these practices provide a strong motivation for interested viewers, for example, expatriates or professionals and students interested in other cultures and societies, to circumvent this obstacle by having recourse to illicit devices. The revenues resulting from the sale of these illicit devices are diverted to the pirates and not to the broadcasters and the right holders. Normal anti-piracy countermeasures disabling pirate cards do not reduce piracy abroad, because non-residents using pirate cards cannot procure valid smart cards by legitimate means and have to turn to pirates if they want to continue watching national television. These business models stimulate the demand for illicit cards, foster piracy, provoke law-abiding citizens to infringe the law, and deny the existence of the internal market.

The clearance of rights on a strictly national basis has also been the subject of work in the context of Directive 93/83/EC on the co-ordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission.[55] Pay-TV services are just the simplest case of cross-border provision of satellite TV. Right holders negotiate with broadcasters the terms and conditions related to the broadcasting of their works. Remuneration is often related to

---

53 http://europa.eu.int/comm/justice_home/funding/agis/funding_agis_en.htm

54 Concerning the "right to use a satellite dish", the Commission has adopted a Communication on the application of the general principles of free movement of goods and services – Articles 28 and 49 EC; (COM(2001) 351 final of 27.06.2001); http://europa.eu.int/comm/internal_market/en/media/satdish/index.htm

55 OJ L248 of 06.10.1993, p.15; see http://europa.eu.int/comm/internal_market/en/media/cabsat/index.htm

the expected audience. By using conditional access technologies, it is perfectly possible to determine exactly what the audience is outside the original territory (the service provider knows to whom – number and place of residence - he has sold his cards) and to collect the fees from the viewers (they bought a card). Conditional access allows broadcasters to serve non-resident clients and to compensate right holders.

Prevention and clever efforts to neutralise potential piracy opportunities lead not only to a *de facto* reduction in piracy but also increase the credibility of appeals for stronger legal protection against the remaining piracy.

The Commission has already publicly announced that it is in the process of reviewing the different aspects of this problem in an attempt to reconcile in a transparent and balanced way the different interests, including the right to fair remuneration of right holders, the business practices of the satellite television broadcasters and the fundamental freedoms of the Treaty.[56]

The Commission calls upon the providers of electronic pay services to actively seek ways to prevent and reduce piracy, for example, by developing together with right holders contractual solutions to provide legitimate non-resident subscribers access to protected electronic pay services under reasonable, non-discriminatory and transparent conditions if those services are by their inherent nature available throughout the internal market.

5. OTHER LEGAL DEVELOPMENTS AFFECTING THE PROVISION OF CONDITIONAL ACCESS SERVICES

5.1. The adoption of Directive 2001/29/EC on copyright in the information society

The adoption, after three years of thorough discussion, of Directive 2001/29/EC[57] in May 2001 marked a major milestone in the process of making the cross-border trade in copyright-protected goods and services easier. This Directive, which is currently being implemented by the Member States, complements the legal protection offered by the Conditional Access Directive, in particular by providing legal protection of anti-copying devices and right management systems. It meets some of the concerns expressed by right holders with regard to the lack of protection under the Conditional Access Directive.

Irrespective of the current scope of application of Directive 2001/29/EC, certain recent technical developments and business models may have to be taken into account in the long term.

Initially, conditional access technologies protected only the signal as transmitted by the service provider. The new generation of in-home digital networks and personal video recorders maintain the conditional protection in the subsequent stages of digital

---

[56] The recent Commission Report on the application of the Satellite Broadcasting and Cable Retransmission Directive (93/83/EC) concludes that the freedom of reception and transmission of TV programmes from other Member States see their effect diminished if the difficulties involved in transferring copyright and related rights are not resolved: COM(2002)430 final of 26.07.2002

[57] OJ L167, 22.06.2001, p. 10.

consumption.[58] Conditional access tends to become part of a larger protection scheme designed to provide end-to-end protection for content in all processes from the point of initial distribution through to the point of viewing and listening by the end-user.[59] Conditional access and digital rights management may use the same encryption engine in the home multimedia centre.[60]

At the same time, business is seeking new ways of exploiting available technologies, in often unexpected and innovative ways, in an attempt to offer new compelling content and to optimise value creation and revenues.[61] These new business models are often experimental, at least in the beginning, and ignore the applicable legal framework.

This technological convergence does not necessarily and automatically have to result in legal convergence, such as merging several legal protection instruments into one single instrument.[62] However, market developments have to be monitored closely in order to ensure that seamless, complementary protection is offered by the law. Conversely, over-protection has to be avoided in order not to stifle innovation and economic development or unduly limit user rights, including fundamental rights such as the freedom of expression or the right to privacy and to protection of personal data.

In the light of these legal, market and technical developments, the Commission considers it is not the right time to propose an extension of the scope of legal protection offered by the Directive to the use of conditional access for copyright reasons.

5.2. The adoption of a new electronic communications services regulatory framework

In March 2002, the Council and the European Parliament agreed on a set of Directives and a Decision laying down the new regulatory framework for electronic communications services and networks.[63] This package was complemented by a Directive on privacy and electronic communications adopted on 12 July 2002.[64]

This package is a major overhaul of the existing Community telecommunications legislation, which further liberalises the markets concerned while adapting rules to

---

58 The new generation of digital video recorders no longer uses video tapes but records directly on hard disk; recorded programmes can only be viewed with a valid smart card.

59 The Digital Video Broadcasting (DVB) Project is currently working on the development of a new integral Content Protection and Copy Management (CPCM) system (www.dvb.org).

60 For more background information and examples see Commission Staff Working Paper on Digital Rights; SEC(2002) 197 of 14.02.2002.

61 Emerging online music services like Pressplay (a joint venture between Vivendi and Sony) are protected by conditional access, but also include rights management of the downloaded or streamed audio tracks. Similar developments exist in video on demand, where premium movies are available on a subscription basis for downloading via the Internet and controlled subsequent viewing, including online, real-time renewal of the subscription after the initial viewing period.

62 See also footnote 10.

63 IP/02/259 of 14.02.2002; Directive 2002/19/EC (Access Directive); Directive 2002/20/EC (Authorisation Directive); Directive 2002/21/EC (Framework Directive); Directive 2002/22/EC (Universal Service Directive), Decision 676/2002/EC (Radio Spectrum Decision); OJ L108, 24.04.2002.

64 Directive 2002/58/EC - OJ L 201, 31.07.2002.

technological convergence. It covers electronic communications networks and services, including networks and services used for broadcasting, and associated facilities. The specific regime for conditional access systems set out in Directive 95/47/EC on the use of standards for the transmission of television signals[65] is also modified.

Under the new electronic communications framework "conditional access systems" qualify as so-called "associated facilities".[66] The requirement to offer access to conditional access services on a fair, reasonable and non-discriminatory basis and interoperability requirements for conditional access that were first set out in Directive 95/47/EC[67] have been carried over in the new framework, though subject to amendment.[68] In particular, conditional access to digital radio services is now covered and market analysis procedures to review obligations in relation to conditional access to digital broadcasting services have been introduced, which notably allow Member States, under certain conditions, to modify or withdraw access obligations bearing on operators with no significant market power.[69] Conditional access systems and services are not covered by the Authorisation Directive.[70]

Whilst not offering legal protection against piracy of conditional access services, this pro-competitive framework governs the provision of electronic communication networks and services in general and conditional access systems in particular, and is as such very important for the further development of the market in the coming years.

The Commission will closely monitor future developments on the conditional access markets under the new regulatory framework for electronic communications when determining whether additional anti-piracy measures may be necessary.

5.3. The implementation of Directive 2000/31/EC on electronic commerce

While the definition of information society services has already existed in Community law since the adoption of Directive 98/48/EC,[71] only with the emergence of the e-Commerce Directive[72] have Member States become obliged to introduce a substantial set of rules and regulations related to information society services.

---

65 OJ L 281, 23.11.1995, p. 51 (repealed as from 25.07.2003); http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm

66 Directive 2002/21/EC; OJ L 108, 24.04.2002, p. 33; Article 2(e) and (f)

67 Directive 95/47/EC mandated *inter alia* the use of the Common Scrambling Algorithm administered by ETSI (this algorithm specifies how the decryption engine of the set-top box deciphers the protected broadcast), the possibility to receive free-to-air transmissions and the DVB Common Interface connector (this is a standardised interface between an interchangeable plug-in conditional access module and the set-top box, permitting several different conditional access technologies to be used on the same box).

68 Directive 2002/22/EC; OJ L 108, 24.04.2002, p. 51; Article 24 and Annex VI.

69 Directive 2002/19/EC; OJ L 108, 24.04.2002, p. 7; Articles 2(a), 6 and Annex I.

70 Directive 2002/20/EC; OJ L 108, 24.04.2002, p. 21; Recital 6.

71 Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations; OJ L 217, 05.08.1998, p. 18.

72 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal market (Directive on electronic commerce); OJ L 178, 17.07.2000, p. 1-16.

Implementation of the e-Commerce Directive will boost legal security for business and consumers and favour the rapid development of all kinds of new interactive services over the Internet, including those protected by conditional access and provided against remuneration.

With the implementation of the Conditional Access Directive most Member States have already introduced the concept of "information society services" into their legal systems. In order to maintain legal certainty, Member States should not introduce different or conflicting definitions in their national legislation.

The e-Commerce Directive provides *inter alia* for a set of common rules limiting the liability of certain intermediary service providers, such as, for example, providers of hosting services.[73] These rules cover liability for all types of illegal activities initiated by third parties online, including the dissemination of piracy-related information or even illicit devices via web sites, news groups and message boards.[74]

The Commission will ensure that any further initiative relating to Conditional Access will be consistent with the e-Commerce Directive.

5.4. The proposal for a Council Framework Decision on attacks against information systems

Recently, the Commission adopted a proposal for a Council Framework Decision on attacks against information systems.[75] This proposal seeks to approximate criminal law across the EU to ensure that Europe's law enforcement and judicial authorities can take action against the new most significant forms of criminal activity against information systems , , aims to supplement what has already been achieved in the field of Community law to protect information systems and is without prejudice to Community law.[76]

The proposed Framework Decision covers *inter alia* the unauthorised access to a computer or networks of computers, including the access to services protected by conditional access without payment. The proposal recognises that conditional access devices, such as digital set-top boxes and personal video recorders, are *de facto* "computers" and that conditional access-protected services are provided via an "information system".

If the approach proposed by the Commission will be retained by the Council, Member States shall bring into force the necessary measures aimed at establishing the offence of illegal access to information systems, if committed against an information system which is subject to specific protection measures (for example, a satellite pay-TV service using conditional access), or with the intent to cause damage (for example, to the provider of conditional access technology or services), or with

---

73 Article 14(1) of the e-Commerce Directive exonerates intermediary service providers storing publicly available information provided by their customers (so-called hosting) from liability for the information stored if certain conditions have been met.

74 Particularly important are the procedures to "take down" material once the ISP concerned has been put on "notice" that it may be unlawful. The e-Commerce Directive does not regulate these "notice and take down" procedures, but it does provide a framework for developing self-regulatory solutions.

75 COM(2002) 173 final of 19.04.2002.

76 See in particular Article 47 EU, Recital 18 of the draft Framework Decision and COM(2002) 173 §1.6.

the intent to result in economic benefit (for example, by making profits from selling illicit devices).[77] The proposal makes no distinction between committing this offence for private or commercial purposes, and does not require that the service is provided for remuneration. Nor does it require that the conditional access systems must always have been bypassed for the offence to have been committed.

The proposed Framework Decision complements the legal protection offered by the Conditional Access Directive and provides an additional level of protection against the piracy of conditional access-protected pay services.

6. COMBATING PIRACY – A PAN-EUROPEAN EFFORT

6.1. Recommendation No R(91)14 on the legal protection of encrypted television services

Back in September 1991 the Council of Europe adopted a Recommendation on the legal protection of encrypted television services.[78] This Recommendation has been the source of inspiration for legislators in many European countries.[79] It has provided a stepping stone towards both the EU Directive and its counterpart, the European Conditional Access Convention.

The Recommendation represents the first generation of legal protection. . It protects exclusively television services using encryption techniques and does not distinguish between pay and free services or between the different reasons for using encryption.

Interestingly, the Recommendation notes that providers of encrypted TV services have the responsibility to use the best available encryption techniques.

Under the Recommendation, all commercial and private activities related to the manufacturing, import, distribution and commercial promotion of decoders enabling access outside the audience determined by the service provider are considered unlawful. Possession for commercial purposes is also considered unlawful, while the unlawfulness of private possession is left to the discretion of individual member states.

The Recommendation insists on appropriate penal or administrative sanctions as well as on the forfeiture of seized decoders and the financial profits resulting from the unlawful activities.

Time has shown that the Council of Europe's pioneering efforts to complement technical protection by legal protection has been instrumental in the consensus-building among European countries on how to effectively tackle piracy.

---

77 Draft Framework Decision, Article 3.

78 http://cm.coe.int/ta/rec/1991/91r14.htm

79 On the basis of this Recommendation, legislation protecting encrypted TV services was enacted in the early 1990s by a number of countries, such as Denmark, Finland, France, Ireland, the Netherlands and the United Kingdom.

6.2. European Convention ETS No 178 on the legal protection of services based on, or consisting of, conditional access

In response to increasing piracy, the Member States of the Council of Europe proceeded in parallel with the adoption of the Directive with negotiations on a similar, binding instrument. The Commission negotiated this Convention on behalf of the Community and its Member States on the basis of a mandate provided by the Council on 12 June 1999.

When negotiating the Convention, the Commission paid particular attention to keeping the Directive and the Convention as closely aligned as possible. The Convention covers more or less the same ground as the Directive and, makes explicit provision for the European Community to accede to it..

Since the opening for signatures on 24 January 2001 the Convention has been signed by three EU Member States and by three Candidate Countries.[80] So far, Cyprus and Romania have formally ratified the Convention. Other Candidate Countries have expressed their intention to accede to the Convention. The Convention requires the consent of three States in order to enter into force.

In order to provide for a coherent pan-European legal framework and an equal level of protection against piracy in the whole of Europe, it is important that Council of Europe Convention No 178 should enter into force as soon as possible. The Commission will work towards ratification of this Convention.

6.3. The legal situation in the other European countries

Pursuant to the provisions of the Agreement on the European Economic Area, the EEA Joint Committee decided on 28 February 2001[81] to incorporate the Directive in Annexes X and XI to the Agreement. This Decision entered into force on 1 October 2001; practical implementation is governed by the EEA rules and procedures. Of the three participating non-EU states, only Liechtenstein has not yet adopted any implementation legislation. Norway has signed Council of Europe Convention No 178 and has amended its Penal Code accordingly.[82] Iceland has amended its media legislation.[83]

Switzerland has signed Council of Europe Convention No 178 and is currently preparing formal ratification and national implementation.

San Marino, Monaco and Andorra have no specific legislation in the field of the Directive. The lack of adequate legislation may result in holes in the pan-European fabric of legal protection against piracy and risks undermining legal protection by creating safe havens for pirates.

---

80 For the full text of the Convention, the Explanatory Report and the most recent state of play concerning signatures and ratification see: http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=178&CM=8&DF=

81 Decision No 17/2001 of 28.02.2001; OJ L 117 of 26.04.2001, p. 21.

82 Norwegian Penal Code, Article 262 in force since 01.08.2001.

83 Broadcasting Act No 53 of 17.05.2000.

The Commission encourages countries which will not be members of the enlarged European Union to join the Community efforts towards an equal level of protection against piracy for the whole of Europe..

6.4. European Convention ETS No 185 on cybercrime

In order to pursue a common fight against cybercrime, the Council of Europe prepared a Convention on cybercrime, which has been open for signature since 23 November 2001.[84] At the date of this report, this Convention has been signed by 13 EU Member States and several Candidate Countries as well as a number of other states.

The Convention obliges acceding countries, *inter alia*, to make the illegal access (hacking) to information systems and, more importantly, the misuse of devices a criminal offence under their domestic laws. The provisions on the misuse of devices, as laid down in Article 6 of this Convention, prohibit the conventional range of activities (e.g. manufacturing, sale, distribution, possession, etc.) related to devices as well as computer passwords and access codes, and are of particular interest due to their scope and generic nature as well as their potential for stopping Internet-related piracy.

The participation of non-European countries holds out the promise of global solutions, which is particularly important for combating Internet-related infringing activities. Transatlantic co-operation on the implementation and the enforcement of the conditional access-related anti-piracy provisions of the Convention should be further explored and if possible extended to other forums.

While the Community cannot accede to this Convention, its solutions in conditional access-related matters should be taken into account and possibly used as a model for further anti-piracy developments within the EU.

7. FINAL CONCLUSIONS AND NEXT STEPS

7.1. Electronic pay services are important for a maturing knowledge economy

Today, electronic pay services exist predominantly in the field of digital pay TV. A massive proliferation of all sorts of new electronic pay services provided over all possible distribution networks is generally expected to happen during this decade. The first examples of subscription-based information society services delivering premium content over the Internet have recently emerged. The digitalisation of cable networks as well as the introduction of digital terrestrial television, 3rd generation mobile communications and advanced transport-related services will result, in the not too distant future, in large-scale deployment of intelligent appliances able to handle pay services. New consumer electronics, such as integrated home entertainment centres and personal video recorders, will be designed to enhance listening and viewing experiences even if conditional access technologies are used and full access is only possible with payment.

---

84 For the full text of the Convention, the Explanatory Report and the most recent state of play concerning signatures and ratification see: http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=

The knowledge-based economies of the 21st century are expected to rely progressively on pervasive electronic pay services. Consequently, the economic and societal relevance of these services will grow over time. Fraud and piracy related to pay services will tend to develop at the same speed as the pay services themselves unless adequate legal protection and effective enforcement is ensured. Piracy of electronic pay services has the same detrimental effects in the knowledge society as white-collar crime and counterfeiting of goods in the 20th century. This development has to be taken into account if the Union wants to meet its ambitious target of becoming the most dynamic and competitive economy by 2010.[85]

It is therefore important to give a clear signal to business and citizens indicating that the Community and its Member States cannot accept that the Union's economic and societal development being severely hindered by acts of piracy and have to take action in the public interest. An early and powerful signal may prevent a level of tolerated and socially accepted piracy, as is currently noticed in the field of digital music.

The Commission considers electronic pay services to be a pivotal building block of the emerging knowledge-based economy. Legal protection against piracy of electronic pay services is an essential condition for the development of such services and a prerequisite for future growth and prosperity for the citizens of the Union.

7.2. Consolidating current legal protection – action to be taken

In its current form the Directive already provides a substantial level of legal protection against the piracy of electronic pay services protected by conditional access. However, as shown by this report, there still is room for improvement in the actual legal protection without amending the Directive itself.

Implementation has not yet been fully achieved within the enlarged Union and enforcement at national level has to be consolidated. Industry and enforcement authorities should continue to develop their public-private partnerships in a combined effort to curb piracy, possibly supported by EU resources.

Successfully combating piracy also includes active prevention and pre-emptive efforts to reduce grey areas where piracy may flourish. Access to protected satellite pay TV by non-resident paying viewers should be made possible.

Only if pirates do not find safe havens in Europe will it be possible to effectively combat piracy. Rapid entry into force of Council of Europe Convention No 178 will contribute significantly to achieving this objective.

---

[85] Lisbon European Council, 23-24 March 2000; Presidency Conclusions, section 5.

Summarising, the following action can be taken to strengthen the effect of the Directive:

- The Commission will vigorously pursue its efforts to have the Directive fully implemented. It will work together with Member States and Candidate Countries to ensure full implementation of the Directive and to clarify all remaining legal uncertainties. If necessary, the Commission will commence infringement proceedings.

- The Commission will consult Member States on the practical difficulties they encounter when enforcing the national provisions to implement the Directive.

- The Commission will encourage industry and national authorities to engage in joint efforts to fight piracy as efficiently and effectively as possible.

- The Commission will continue to co-operate with other European countries and the respective international organisations in order to enforce coherent application of European rules against the piracy of electronic pay-services.

- The Commission recommends right holders and service providers to actively seek contractual solutions to provide legitimate non-resident subscribers access to protected electronic pay services under reasonable, non-discriminatory and transparent conditions throughout the internal market. The Commission will contribute to this process in the context of its review of Directive 93/83/EC.

7.3. Enhancing legal protection – what next?

The piracy of electronic pay services protected by conditional access is a cyber crime which has changed significantly in recent years. While current legal protection is quite effective against conventional forms of piracy, protection may have to be enhanced in order to be able to cope with the new categories of offenders, the effects of the Internet and some remaining enforcement issues.

Given the estimated protection potential of additional measures based up the current Directive, the Commission holds the view that it would be premature to propose amendments to the Directive on the basis of this Report, but that a revision of the Directive might be considered in the context of a coherent set of legal measures against all possible forms of piracy.

However, the consultations and assessment undertaken in the context of this Report have enabled the Commission already to identify the following issues, which deserve further reflection in close co-operation with the Member States and industry:

- Industrial forms of piracy are clearly commercial and therefore already covered by the Conditional Access directive. This type of piracy is very similar to the counterfeiting of goods or copyright-related piracy. A balanced and coherent enforcement framework applicable to all kinds of piracy and counterfeiting and agreed at Community level would bolster the effectiveness of the legal protection of electronic pay services.

- Arguments have been advanced that casual pirates and individuals pirating solely for their own purposes could be prosecuted, including for infringing activities

which are not undertaken for commercial purposes and/or for the private possession of illicit devices. However, an extension to the Conditional Access directive along these lines would imply a fundamental change in Community policy and may have an impact on adjacent legislation.

- The current Directive is not very effective against those forms of piracy which have emerged as a result of the Internet. One way of fighting these forms of piracy is to prohibit the direct and indirect distribution of keys and illicit devices via the Internet, backed up by a notice and take down remedy for affected service providers. Such a prohibition/remedy targets the principal source of many piracy acts and may avoid other measures that are more invasive to private individuals. Article 6 of the Council of Europe Convention on Cybercrime already presents a model for such a measure. In this context the Commission does not envisage any measure restricting the dissemination of detailed technical information on conditional access systems, because this would unduly limit the freedom of expression and stifle innovation.

The Commission will continue its examination of the application of the Conditional Access directive and its relationship with other provisions of Community law, including whether or not there is a need to amend the Directive. It invites Member States, Candidate Countries and other interested parties to contribute to this exercise.