



Hacking BskyB: The legal protection of conditional access services under European law

Published in *Entertainment Law Review*, 1999-5, p. 88

Natali Helberger

Within Europe, the legal protection of pay-TV services against piracy is not as complete as service providers might hope. This article explores to what extent the recently adopted Conditional Access Directive will change this situation.

Introduction

Is it unlawful to hack BskyB? Pay-TV channels such as BskyB are part of an increasing number of electronic services which are offered on the basis of conditional access techniques. By applying these techniques, the broad audience is excluded from receiving the contents. Instead, services are delivered upon prior individual demand, mostly combined with the obligation to pay a fee.

Not surprisingly, services based on electronic access control inspire an increasing number of technical experienced people to circumvent the technology, and to access the service with neither authorisation nor remuneration. Moreover, the increasing availability of pirate cards, decoders and instructions on how to access a pay-TV channel is symptomatic of the development of a flourishing market in commercial piracy equipment.

Piracy of conditional access services can cause considerable commercial harm, such as the loss of profits, additional costs for replacing the system and the waning confidence in the security of such systems. However, the legal protection of conditional access services suffers from an appreciable lack of legal certainty. Only a small number of Member States have adopted specific regulations^[1], and these differ widely in scope and enforcement.^[2] Furthermore, existing laws are far from providing an overall protection scheme, since many cases in an electronic environment are not covered. Where specific regulations are absent, national courts generally apply existing general laws of unfair competition, copyright and penal laws - as far as they are applicable. One consequence of this is that the legal protection of service providers is here subject to the individual interpretation of national courts, and there may be considerable differences in outcome. Since electronic services are no longer bound to the territory of one Member State, the existing differences within the Community make it extraordinarily difficult to say whether in a concrete case the hacking of conditional access systems is unlawful or not.

The European Commission recognised the economic significance of conditional access services to the Internal Market.^[3] In its Green Paper on the legal protection of encrypted services^[4], the

Commission also came to the conclusion that existing differences in the applicable protection schemes for technical devices within the Member States were one cause of the problem piracy. By presenting a Directive on the legal protection of services based on, or consisting of, conditional access, the Commission intended to establish a harmonised level of adequate legal protection for such services.^[5] The Directive has recently been adopted, and came into force on the day of its publication - 28 November 1998 - in the Official Journal of the European Communities.^[6] From that date on, all Member States will have to implement the directive into national laws, regulations or administrative provisions by the 28 May 2000.

This paper outlines the scope of and background to the proposed directive. It also devotes consideration to the forthcoming implementation through the Member States. Furthermore, it examines whether the directive provides an adequate instrument to combat piracy in the electronic environment.

Conditional access

Pay-TV services are probably the most well-known services based on conditional access. But on the Internet, too, service providers increasingly use conditional access techniques to provide online access to databases, to deliver music and video clips on-demand or to trade electronic newspapers.

The significant feature of a service based on conditional access is that consumers will have to go through an electronic authorisation process before being supplied with the requested content. By means of electronic access control service, the provider prevents persons other than those duly authorised end-users access an electronic service.

The conditions for gaining authorisation depend on the purpose served by access control. As this will be - in the majority of cases - the profit-making of the service provider, a consumer will have to pay a certain fee or remuneration.

The conditional access system itself generally consists of several technical and consumer-orientated components, which can be offered by competing providers. The provision of conditional access to services therefore requires a vast service infrastructure consisting of various activities such as subscriber management and authorisation services, packaging and encryption services, as well as the manufacturing of the required hard- and software.^[7]

Conditional Access Directive

According to Article 1 of the Conditional Access Directive, the directive intends to "approximate provisions in the Member States concerning measures against illicit devices which gave unauthorised access to protected services."^[8] In pursuit of this objective, the directive bans selected activities facilitating the circumvention of conditional access devices used in services protected.

Scope

Protected services are not only broadcasting, i.e. pay-TV services, but also radio broadcasting as well as so called Information Society Services that are offered on the basis of conditional access and against remuneration.

The term "Information Society Services" was introduced as a legal concept in the Commission's proposal for a Directive amending Directive 83/189/EEC concerning the "regulatory transparency in the Internal Market for Information Society Services".^[10] In its Article 1 the Directive defines Information Society Services as

"any service normally provided for remuneration, at a distance, by electronic means and on the individual request of a recipient of services" , irrespective of whether the receiver uses a television set, a computer screen or any other equipment".^[10] The term covers not only online services but also services which are not considered to be neither broadcasting nor online services.

No Information Society Services are traditional telecommunication services, for telecommunication services are not provided "by electronic means", i.e. they are not provided via electronic processing systems.^[11] Therefore the directive does not apply e.g. to a pin code system of a mobile phone. However, regarding the ongoing convergence it will be difficult to draw a line between Information Society Services and telecommunication services. An increasing number of telecommunication companies expand their offer on the provision of additional value-added services such as information services, alarm calls, hotel reservation, platforms for video conferences or even travel pilot services. Since these services are offered upon individual request, on a distance and by electronic means it could be argued that these services also qualify as Information Society Services as protected under the directive.^[12]

By including Information Society Services, the Directive goes further than most of the existing national regulations which are generally confined to broadcasting services. Only a few Member States such as the Netherlands, Finland, the United Kingdom and Sweden have also included services other than broadcasting in their protection schemes.

A consequence of the wide scope of the term "Information Services" and the unrestricted protection under the Directive is not only the uncertainty of the definition itself but also that service providers are invited to commercialise practically any content since nearly all services available upon individual request by electronic means will be protected. This possible effect of the directive would correlate with the intention of the directive to promote the development of a market for commercial electronic services.

Conditional Access

Article 2(b) of the Conditional Access Directive defines "Conditional Access" as

"any technical measure and/or arrangement whereby access to the service in an intelligible form is made conditional upon a prior individual authorisation."

Note that "any technical measure" or "arrangement" is protected, irrespective of whether it is effective or not.^[13] This is to avoid excluding smaller service providers from the protection under this directive, particularly if they cannot afford the installation of costly solutions.^[14]

It is important to notice, that the Directive probably does not consider a wide range of other reasons for controlling access such as security, privacy, integrity or copyright protection.^[15] Clearly, such reasons were excluded in an earlier version of the definition of conditional access, which stated more precisely that conditional access are considered such measures/arrangements "aiming at the remuneration of that service".^[16] However, this addendum has been omitted in the final version of the directive. Therefore, it remains open to

doubt whether under the final version of the directive also measures serving other purposes than ensuring adequate payment are considered conditional access. In this case, also the circumvention of conditional access techniques serving other interests such as the confidentiality and exclusivity of the service might fall within the scope of the directive (as long as the service itself is offered against remuneration)^[17].

The directive does not define the term "remuneration". Considering, that the existence of an "remuneration" interest is used as an important criterion whether the Directive applies, this could lead to difficulties in determining who is entitled to protection under the directive. "Remuneration" of an service could be understood as the payment a service provider obtains directly from the customer in exchange for services. The term also could be understood in a broader sense as any financial profit a provider of services gains, directly or indirectly and irrespective from whom, such as commissions, brokerages, maintenance's or rewards and prizes. The existence of a precise definition may become relevant for arrangements such as an electronic online catalogue where the service itself is offered to the user free of charge, but the provider of the catalogue is remunerated by the advertiser.

Encryption not required

As far as specific national anti - piracy regulations exist, they consider mainly encrypted services. Service providers using other techniques are not protected insofar. Also the Green Paper dealt exclusively with encrypted services, whereas the legal protection under the Conditional Access Directive is not made conditional upon the prior encryption of the transmitted signal. The Conditional Access Directive will also apply to scrambling and other techniques such as electronic locks and passwords.^[18]

By taking in account that conditional access services are not merely confined to encryption technologies, the Commission leaves room for future technological developments. Moreover, the Conditional Access Directive seeks to extend the scope of protection to a considerable number of services which limit access without using encryption techniques. If the Conditional Access Directive is to be adopted, national regulations such as in France and the United Kingdom, which are limited to encrypted signals, will have to be amended.

Conditional access as a service in its own right

It is remarkable that the Conditional Access Directive considers also the provision of conditional access as "a service in its own right".^[19] Providers of conditional access to services will benefit from the same legal protection than providers of electronic services.

The Conditional Access Directive does not precisely defines what functions of a conditional access system fall under the directive. As mentioned above, the provision of conditional access can be connected to a wide range of services in its own right. Covering each supplier of the technology would lead to an extensive number of beneficiary. To avoid an unreasonable number of potential plaintiffs and a disproportional protection of the suppliers of conditional access technology, national legislators will have to refine the definition of conditional access as a service in its own right.

Unlawful activities

As a main statement Article 4 requires Member States to take all measures necessary to prohibit on their territory a number of activities that favour and allow for the circumvention of

conditional access services such as:

- the manufacture, import^[20], distribution, sale, rental or possession for commercial purposes of illicit devices;
- the installation, maintenance or replacement for commercial purposes, of an illicit device;
- the use of commercial communications to promote illicit devices.^[21]

The listed activities have in common that they all are preparatory activities facilitating the circumvention of conditional access systems. The unauthorised access itself is not unlawful under this directive. Consequently, private acts of circumvention do not fall within the scope of this directive. Unlike the European approach, the laws of a considerable number of Member States including Ireland, Italy, the French Community in Belgium, the United Kingdom and Finland consider the unauthorised access as such as unlawful. As a consequence, the laws of these countries ban additionally the application of illicit devices in order to access a service without paying for it, whereas under the conditional access directive, unauthorised access to services remains lawful.

For commercial purposes only

Significantly, the Directive concentrates on commercial infringing activities.^[22] Consequently, the Conditional Access Directive does not prohibit attempts to circumvent conditional access barriers for private purposes. Therefore, the offering of a decoding programme to the public on a homepage is not unlawful, as long as this will happen in most of the cases free of charge.^[23] The directive does not prohibit to follow such instructions and construct private pirate cards, too. Also the private downloading of illicit information or programmes is not forbidden - not even if they are obtained for the purpose of commercialising the information again e.g. by selling them to third persons. This does not mean that hacking of electronic services for non-commercial purposes is generally lawful under existing applicable laws. Some Member States, including Great Britain, Ireland, Italy, Belgium and the Netherlands also ban private acts of circumvention. Under the Conditional Access Directive, the European Commission leaves it open to the Member States to consider also private behaviour as unlawful^[24], when implementing the directive.

As the European Commission explains, Article 3b of the European Treaty limits Community actions to what is necessary to achieve the pursued objective.^[25] However, since the non-commercial circumvention of conditional access systems can incur as many costs and damages as commercial activities, particularly if it is linked with the publication of hacking programmes or passwords, and given the substantial number of persons having illicit access to protected services in this way, it is questionable whether the concentration on commercial activities is suitable for achieving the objective of the proposed Directive. Furthermore, commercial piracy activities generally will fall under national unfair competition law. Therefore, a need for specific legislation appears to exist especially in respect to private events of circumvention.

Illicit devices

"Illicit devices" means :

"any equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorisation of the service provider".^[26]

It is notable that the equipment or software itself is not considered illicit as far as it not

"designed or adapted to give access ... without authorisation". The Conditional Access Directive introduced an element of purpose, probably in order to prevent hampering the general equipment market. Additionally, national legislators are left free to provide that the activities, addressed in Article 4 of the Conditional Access Directive, have to be carried out in the knowledge or with reasonable grounds for knowing that the devices in question were illicit.^[27]

The definition of "illicit devices" includes pirate cards and the various programs for replacing passwords. An interesting question is whether the password itself can be considered as an "illicit device", in a situation where the user is not legitimated to use the password. The password is neither equipment nor software. It is information needed by the equipment or software to allow access. As the wording of the activities listed in Article 3 of the Conditional Access Directive shows, the European Commission refers exclusively to apparatus which can be used to circumvent conditional access technologies. In concentrating on the commercial decoder business the European Commission follows the approach of the Council of Europe to ensure that only preparatory activities related to the unauthorised access to signals and not the access itself are prohibited.

Given the limitation on the commercial decoding business it remains unclear whether the Conditional Access Directive is suitable to provide an adequate legal protection to online services. Online services which are based on conditional access generally do not require the application of any hard- or software in order to access the service, but instead involve the feeding into the system of a password or a credit card number. As a result, most of the online services might be not protected under this Conditional Access Directive.^[28]

Some national laws, such as the Dutch Penal Code, go a step further by explicitly prohibiting the abuse of passwords.^[29]

Sanctions and remedies required

The real value of regulation depends on the sanctions and remedies provided herein. As far as specific national regulation exists, the current legal situation in Europe is characterised by a range of different administrative or civil sanctions^[30] such as the forfeiture or seizure of prohibited decoding equipment and the economic profit gained, and such additional sanctions as prison sentences^[31] and fines.^[32] Service providers may also claim compensation or request an injunction. The set of sanctions and remedies available depends on the applicable law. The same is true for the conditions under which remedies and sanctions are granted.^[33]

Sanctions

Rather as a matter of course than an obligation Art. 5 (1) of the Conditional Access Directive states that sanctions are to be "effective, dissuasive, and proportional to the potential impact of the infringing activity".^[34] Obviously, the European Commission did not intend to fix a harmonised level of penalties. The vague wording leaves considerable freedom to the national legislator to decide what sanctions are adequate and in which field of law they are to be introduced.^[35] The European Commission merely proposed to take into account the TRIPS Agreement^[36], which indicated a comprehensive set of measures against piracy.^[37] It should be born in mind, that the TRIPS Agreement refers exclusively to civil and administrative sanctions, whereas most of the existing specific laws are adopted in the field of criminal law^[38].

Remedies

Additionally, Art. 5 (2) obliges Member States to take the measures necessary to ensure that service providers, whose interests are affected can bring an action for damages and/or apply for an injunction and, where appropriate, "for disposal outside commercial channels of illicit devices"^[39] the seizure of illicit devices.

Clearly, Art. 5 (2) CA focuses on civil and administrative remedies^[40] only, not considering penal sanctions.^[41] The directive aims at the realisation of remuneration claims, which is usually not provided for by criminal law. Therefore, a transformation, though not expressly excluded^[42], of the directive into criminal law probably would fail to meet the requirements of the directive. As a consequence, those Member States who apply special or general provisions of their penal codes to cases of piracy may have to adopt additional civil legislation.

Right to take action

One of the most controversial issues is the question of who is entitled to bring an action under this directive. According to Art. 5 (2) of the Conditional Access Directive this right is available to service providers, whose "interests are affected by an infringing activity". The directive addresses exclusively providers of broadcasting and Information Society Services and the providers of conditional access to such services. The exclusion of other parties, especially rightholders, who are detrimentally affected, has been the target of several criticism. In its recent opinion on the directive, the Economic and Social Committee proposed to expand the right to institute proceedings to anyone who can prove a direct interest.^[43] The Committee on Legal Affairs and Citizen's Rights explicitly proposed including copyright owners.^[44] The European Commission explains that "though from an economic point of view, rightholders will certainly benefit from such measures, this will be an indirect effect, and their interests remain distinct. The same reason applies to the issue of industrial property rights for conditional access devices."^[45] Against this assumption it has been argued correctly that rightholders do have an interest in a proper exploitation of contents and that there is not always an identity of interests between service providers and those who own rights in the material transmitted. As a result, rightholders might find themselves unable to enforce their interests against the effects of the illegal use and possible retransmission of creations. On the other hand, one could also argue that potentially affected interests of rightholders and third persons should remain subject to contractual solutions. However, it is notable, that most national regulations grant legal remedies to anyone whose rights are affected.

Legal protection is made conditional upon the proof of the infringement of an interest as protected under the directive. In case of the provider of the conditional access service this is the remuneration interest of the service provider. Since the remuneration interest refers exclusively to the relation between service provider and (unauthorised) user, it is not clear under which conditions the provider of conditional access as a service in its own right might claim for damages. However, a selective definition of protected interests with respect to the providers of access control services might serve as an additional criterion to limit the number of potential plaintiffs in the case of circumvention of a conditional access system.

Cross-border aspects

The jurisdiction of each Member State applies in relation to acts of infringement undertaken within their territory. It was not clear under the Conditional Access Directive whether the state in which an infringement of the provisions of the directive was committed had to grant access to its national courts to affected service providers of other Member States, especially if the foreign service provider have no programming rights on the foreign market.^[46] For example, the United

Kingdom offers protection against the unauthorised reception of services transmitted from a state other than the United Kingdom only under the condition that the foreign service provider obtains an order from the Ministry of National Heritage.^[47] The Conditional Access Directive neither states whether access to remedies has to be granted to foreigners under the same conditions as to citizens of the Member State nor which law is applicable in case of infringing activities with cross-border aspects.

Conclusion

The hacking of BskyB is not unlawful under European law. Thus far, the legal situation within Europe remains unclear. However, as a result of the directive, the commercial exploitation of intentional hacking of pay-TV programmes may soon be subject to specialised legislation in all Member States.

It remains open to doubt whether the effect of the directive, when implemented, will exceed the level of protection already provided for under existing applicable national law, especially in respect of the commercial decoder business. Due to the retentive attitude of the European Commission, the directive focuses on setting a common minimum standard of legal protection, which, under existing applicable law, probably already exists. The vagueness of definitions and the restrictive scope of the directive, together with the absence of determination of sanctions and remedies, might even lead to a failure to achieve a harmonised level of protection. From the previous paragraphs, one may also doubt whether the directive, still thinking in terms of broadcasting, will meet the requirements of the Internet and the progressing process of convergence, or whether a technology and service independent approach would not have been more practicable.

Finally, the effect of the directive will depend to a considerable extent on the way in which the national legislatures decide to translate the regulation in practice. As far as is known, all Member States will have to adopt new or adapt existing legislation to meet the requirements of the directive. Whereas the Directive focuses on sketching a future European protection scheme, the European Commission leaves considerable freedom to Member States to design the details. Due to this regulatory retention of the European Commission, Member States will have appreciable influence on determining the final scope and impact of the directive. Apart from refining the key definitions introduced by the directive, several decisions will have to be taken, such as the treatment of non-commercial behaviour, the choice of the appropriate field of law^[48], the lawfulness of unauthorised access itself and the choice of adequate sanctions and remedies.

The task of creating an appropriate legal scheme for the protection of conditional access services is rendered difficult by the fact that the debate on the legal protection of technical measures in general and conditional access techniques in particular is still ongoing. Conditional access is a tool that may serve many different purposes such as to ensure security, privacy, integrity and confidentiality of data and communications, secrecy, confidentiality or rights protection. Moreover, conditional access techniques may develop to an important instrument to enforce rights and contractual obligation in the electronic environment of the future. The European Commission envisages conducting a study on the question of whether or not there is a need to provide for additional legal protection for those services which use conditional access, for reasons other than to ensure remuneration. As a result, in the near future Member States might meet the need to adopt additional protection schemes on the same technology but may differ markedly in terms of conditions of protection and law enforcement.^[49]

However, the significance of the directive probably goes further than banning acts of

commercial piracy towards electronic services. The European regulation signals that, from an European point of view, the progress of a prospering conditional access market is welcome, and deserves promotion. Otherwise, it would be rather difficult to understand, why the European Commission did not content itself with protecting service providers themselves, but additionally included the providers of the supplying technology within the scope of protection. Moreover, the provision of fee-based services is made increasingly attractive, since the directive protects only the use of technological measures where a remuneration interest of the service provider exists. If the signal is correctly understood, we will probably observe an increasing number of commercial pay-per-content services, not only in the broadcasting sector but also within the Internet. Whereas the Conditional Access Directive focuses on one single aspect of conditional access - the remuneration interest of service providers - it might be time to also take into account the fundamental interests of the users and of society as a whole.

One interest of a constitutional nature, which is certainly affected by the ongoing commercialisation process of the media, is the right to receive and impart information as protected under Article 10 ECHR.^[50]

Article 10 ECHR might raise questions in respect of the extensive protection of providers of conditional access as a service in its own right. In particular, one aspect which is not dealt with under this directive is the question of how to ensure that the operators of access control do not abuse their position through acting "as a bottleneck"^[51] to entry to the electronic service market. For the field of broadcasting services this problem has already been recognised. As a result, the operators of conditional access systems to broadcasting services are obliged under Art. 4 of the Directive 95/47/EEC on Advanced TV Standards^[52] to give access to providers of digital television services on "fair, reasonable and non-discriminatory" terms. However, neither the Directive 95/47/EEC nor any other regulation at European or national level imposes the same obligation upon providers of conditional access to online services. Since the present Conditional Access Directive probably will lead to a considerable promotion of the conditional access market, not only in respect to broadcasting but also to online services, ensuring access may prove to be a crucial issue.^[53] One could argue, that competition laws might provide the appropriate solution in cases of unfair behaviour of conditional access providers.^[54] However, it is doubtful whether existing competition law provides a sufficient instrument to prevent abuse.

In regard to Article 10 ECHR, it has been discussed recently how to ensure that information which is important in respect of the freedom of information is not sold out to the pay-TV market. The Commission states explicitly within the statements that the Conditional Access Directive is without prejudice to possible future Community and national provisions ensuring that a number of public interest broadcasting services are not based on conditional access.^[55] This refers to legislation both at the European level and in certain Member States. This includes the drawing up of lists of events of "major importance for society" on the basis of Art. 3a of the revised Television without Frontiers Directive^[56], including the Olympic Games and major football championships. However, Art. 3a of the revised Television without Frontiers Directive refers exclusively to broadcasting services, whereas free access to certain online contents is (still) not subject to either European or national legislature. Considering its potential impact on the process of opinion-forming, Art. 10 ECHR might request similar protection schemes for the Internet.