CTB(CR) 9/19/1 (03) Pt. 23
CB1/BC/11/01
2189 2236
2511 1458
echeung@citb.gov.hk

2 February 2004

Clerk to Bills Committee
Legislative Council
3/F, Citibank Tower
3 Garden Road
Hong Kong

(Attn: Miss Polly Yeung)

Dear Miss Yeung,

Bills Committee on Broadcasting (Amendment) Bill 2003

We refer to the Hong Kong Cable Television Limited (HKCTV)'s letter of 30 January 2004 to the Bills Committee and would like to provide the following in response.

Availability of digital unauthorized decoders

As pointed out in our letter of 13 January 2004 to the Bills Committee, unauthorized decoders available in the black market at present are mainly those for enabling access to the analogue television service of HKCTV. There is a difference between the fake devices claimed by illicit

vendors as being able to decode the digital service of HKCTV and devices actually designed in an attempt to decode the digital service of HKCTV by circumventing the protective measures to avoid payment of a subscription fee. Of around 1,000 unauthorized decoders seized in the enforcement operations in 2003, only two of them were confirmed as devices able to decode the digital service of HKCTV.

Import and Export of Unauthorized Decoders

The existing section 6(1) of the Broadcasting Ordinance (Cap. 562) prohibits, among others, the import and export of unauthorized decoders in the course of trade or business. The Customs and Excise Department has not detected smuggling of unauthorized decoders for commercial purposes so far.

European Union's Policy

On page 3 of HKCTV's letter, it states that the Government "repeatedly advocates that the European Union (EU) legal instruments require sanctions to be imposed only on commercial activities favouring unauthorized reception, not on unauthorized reception per se. However, it fails to point out to the LegCo Members that it is the policy of the EU to introduce only a minimum level of legal protection against piracy and to grant Member States flexibility to extend the scope of prohibitions to cater to their own needs…."

The European Commission explains the policy objective and application of the EC Directive on Conditional Access 98/84/EC in its Report on the Implementation of the EC Directive on Conditional Access 98/84/EC (EC Report) published in April 2003. Paragraph 2.2.2 of the EC Report clearly states that "[T]he Directive imposes sanctions only on commercial activities favouring unauthorized reception, not on unauthorized reception as such" (page 8 of the Report). It is the unequivocal position of the EU, not the Administration's advocacy as suggested in HKCTV's letter. The Administration quoted the exact

wording of the aforesaid statement in the EC Report in paragraph 5 of the Administration's submission to the Bills Committee (LC Paper No. CB(1)2525/02-03(02)). We welcome the Bills Committee to verify the EU's position on this matter with the European Commission directly, as the Administration has done so when preparing for our submissions to the Committee.

The Administration also faithfully drew Members' attention to the fact that "a minority of [EU] Member States prohibits personal use and/or private possession of illicit devices" (paragraph 3.3 of the EC Report). At the Bills Committee meeting on 7 October, Members specifically asked the Administration how many EU Member states had imposed enduser criminal liability, as recorded in the minutes of the meeting. In reply, the Administration cited Member States such as the UK, France and Italy that have criminalized pirated viewing of pay television service.

Relevant extracts of the EC Report and LC Paper No. CB(1)2525/0203(02) are attached for Members' ease of reference.

Public views

HKCTV also alleged that the Administration played down the support for imposing criminal liability upon illicit domestic endusers from many organizations within and outside the industry.

The fact is that we received about 50 submissions during the public consultation on the proposed legislative measures. About half of the submissions, including those from the Consumer Council, some professional bodies, chambers of commerce, and a District Council, expressed grave reservation about imposing enduser criminal liability. The Administration has reported the outcome of the consultation to the LegCo Panel on Information Technology and Broadcasting and the Bills Committee on several occasions, as recorded in the relevant minutes of

meeting and the Administration's previous submissions. We welcome the Bills Committee to scrutinize the submissions to the public consultation.

Yours sincerely,

(Eddie Cheung)
for Secretary for Commerce, Industry and Technology

Encl.

c.c. Hong Kong Cable Television Limited
(Attn: Mr Eric Lo, Executive Director – Cable Subscription Services)

Attachment

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

TABLE OF CONTENTS

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.

---

12 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.

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.

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).

Broadcasting (Amendment) Bill 2003
Administration's response to issues raised by Members
at the Bills Committee meeting on 10 September 2003

(a) The question of legal inconsistency if abstraction of electricity and dishonest use of public phones are criminal offences while using an unauthorized decoder for domestic viewing of subscription television services without payment of a subscription is not.

Whether or not to criminalize abstraction of electricity, dishonest use of public pay telephone or pirated viewing of pay TV is a policy rather than a legal matter.

2. The Government does not condone pirated viewing which hurts the pay TV industry. The existing section 6 of the Broadcasting Ordinance (Cap. 562) already provides for criminal sanction against commercial manufacturing, distribution and marketing of unauthorized decoders. We consulted the public in late 2001 on whether we should extend the criminal sanction to cover end-users. The views of the public are diverse. Even some respondents who support criminalization in principle consider that the Government should take a cautious approach as enforcement will be intrusive.

Policy Consideration

3. When formulating our legislative proposal, we have taken into account the interests of the industry, the outcome of the public consultation and the adequacy of digitization and conditional access technology to prevent pirated viewing. On balance, we decided to tighten the control of pirated viewing by proposing the extension of the scope of criminal sanction to cover pirated viewing for commercial purposes. We also suggest providing for civil remedy against both domestic pirated viewing and pirated viewing for commercial purposes.

4. At the same time, we encourage and assist pay TV operators, in particular, Hong Kong Cable Television Limited, to digitize their service. If digitization fails to contain the problem, the Government will

consider providing for criminal sanction against domestic pirated viewing.

International Practice

5. Our approach is in line with the practice in many advanced economies. We note that HKCTV has cited examples of criminalization of domestic and commercial pirated viewing in other jurisdictions. In this connection, we wish to draw Members' attention to the Report on the Implementation of the EC Directive on Conditional Access 98/84/EC published on 24 April 2003. The Report states clearly that the Directive "imposes sanctions only on commercial activities favouring unauthorized reception, not on unauthorized reception as such". It also explains that the Directive and Recommendation R(91)14 of the Council of Europe consider that "the most effective way of thwarting piracy is to concentrate on commercial activities enabling illegal access". The Recommendation notes that providers of encrypted TV services have the responsibility to use the best available encryption technology. Moreover, the Report mentions that only "a **minority** of Member States prohibits personal use and/or private possession of illicit devices" (emphasis added) (pp. 8, 10, 13 and 26 of the Report).

6. In Australia, the Copyright Amendment (Digital Agenda) Act 2000 "introduces remedies and offences in relation to the manufacture, sale and other dealings with broadcast decoding devices that facilitate unauthorized access to encoded broadcasts". The provisions do not prevent the personal use of such devices, but a civil remedy is provided for the use of a decoding device for a commercial purpose (for example the unauthorized reception of an encoded sporting event in a hotel or pub) (page 6 of the *Fact Sheet on Copyright Amendment (Digital Agenda) Act 2000* - Attorney-General's Department of Australia).

7. To the best of our knowledge, even in jurisdictions where pirated viewing is criminalized, there has been no active enforcement against domestic pirated viewing. In most cases, enforcement action focuses on the upstream dealer level. For example, in Canada, both the Royal Canadian Mounted Police and the industry suggested that enforcement action should focus on dealer activity in their representations

to the Parliament's Standing Committee on Canadian Heritage (pp. 515 - 516 of Committee's Report *Our Cultural Sovereignty – The Second Century of Canadian Broadcasting*, June 2003).

Conclusion

8. We consider that our gradual, balanced approach is more acceptable to the public and is in line with international practice. If the Bill is passed, there will be enhanced deterrent effect and proportionate protection of the rights of the industry. We also expect that Hong Kong Cable Television Limited will digitize its service as soon as possible and the industry will deploy effective encryption and conditional access measures to contain the problem. We believe this public-private partnership approach is the most effective way to tackle the problem.

9. There are therefore special policy considerations applying to sanctions for pirated viewing of pay TV which cannot be compared on the same basis to other wrongdoings. In any case, we have not ruled out the possibility of criminalization. We only consider that criminalization is the last resort if technological measures fail to contain the problem.

(b) The Bar Association's concern about presumption in the Bill.

10. We have addressed the concern in both our responses to Assistant Legal Advisor's comments and to the deputations' views.

(c) Estimated number of unauthorized decoders currently in use in Hong Kong.

11. Before starting the digitization of transmission, Hong Kong Cable Television Limited (HKCTV) had claimed that 100,000 unauthorized decoders were in use in Hong Kong. These devices are able to facilitate viewing of HKCTV's service in the analogue format only. They are useless in areas where HKCTV's service has been digitized.

12. Unless we conduct a massive on-site inspection and survey we will not able to come up with a guesstimate of the number of unauthorized decoders in use. However, since HKCTV has digitized about half of its service coverage and is required to complete digitization by May 2005, we believe that the number of unauthorized decoders in use for viewing HKCTV's analogue service is very limited and will keep declining in time. Unauthorized decoders, including smart cards, which facilitate viewing of HKCTV's digitized service, even if available in the black market, may not be appealing to buyers because they will be rendered useless once the operators have changed the digital key of the encryption.

(d) Concerns about difficulty in ascertaining the person(s) in domestic premises who should be liable for civil action.

13. Proposed section 7B(3) allows a licensee to bring civil action against any person who possesses or uses, or authorizes another person to possess or use an unauthorized decoder to view any licensed television programme service without payment of a subscription. The standard of proof in a civil action is "balance of probabilities". Given the wide scope of the proposed provision, a licensee may bring an action against any person in the premises for possession or use of the unauthorized decoder. Our policy intent is to facilitate a licensee to take civil action and achieve maximum deterrent effect. We believe that the present wording is adequate for the purposes.

Communications and Technology Branch
Commerce, Industry and Technology Bureau
3 October 2003