



HK Cable Supports Criminalization of Pirated Viewing

- **Pirated Viewing is theft**
 - ◆ *Stealing electricity and fraudulent use of a public telephone without paying prescribed fees are acts of theft and are criminal offences, viewing of Pay TV programmes through devices other than those authorised by the programme suppliers and knowingly escaping payment of fees should be subject to the same sanctions*

- **Why End-user criminal liability is justified**
 - ◆ *Existing legislation which criminalises suppliers, manufacturers and traders of unauthorised decoders is not adequate as they are supplied from sources outside of Hong Kong. Pirated viewing cannot be effectively controlled unless it is sanctioned at the end-user level*

 - ◆ *The problem is severe and has been causing significant damage*
 - * *It is more threatening and damaging than conventional videogram infringement*
 - * *Recurring loss of revenue to Pay TV companies*
 - * *Recurring loss of tax to the Government*
 - * *Recurring loss of revenue to local and international content providers*
 - * *Loss of attractiveness of Hong Kong as a regional broadcasting hub*
 - * *Loss of quality programming and local and overseas investments*
 - * *Hong Kong could become a piracy heaven*
 - * *Children could be easily exposed to unsuitable programmes because unauthorised decoders have no parental lock*
 - * *Parents who use unauthorised decoders could give children a wrong message that greed and dishonesty are acceptable*

 - ◆ *Implementation of the criminal law is not intrusive and there are safeguards against abuse of power by enforcement agency*
 - * *No entry without a warrant issued by court*
 - * *No warrant issued without satisfactory information on oath*
 - * *Penalty for providing false information on oath or abusing power*
 - * *Technical detection of signal theft possible without entering private premises*

 - ◆ *End-user criminal liability targets only the knowing swindlers and does not jeopardize the innocent public*

- **End-user criminal liability is not a new idea**
 - ◆ *In 1993, the Law Reform Commission of Hong Kong recommended that fraudulent reception of a transmission should be made a criminal offence*



- ◆ *At least 12 jurisdictions (including UK, US, France, Canada and New Zealand) have imposed both criminal and civil liabilities at end-user level for pirated viewing (details in the Appendix)*
- **Civil liability alone is inadequate**
 - ◆ *There is no logic (as some people have suggested) that criminal investigation could be more intrusive than civil investigation*
 - ◆ *Collection of evidence by the Pay TV companies themselves could be difficult and dangerous. In the case of domestic premises, the caretakers may expel our investigators at the entrance of the buildings. Public places such as pubs, karaokes and places of entertainment are risky for civil investigators to collect evidence without protection of law enforcers.*
 - ◆ *Civil liability has no deterrent effect*
- **Technological measure alone is inadequate**
 - ◆ *There is no security system which can never be hacked*
 - ◆ *More system modifications mean more business opportunities for the suppliers of unauthorised decoders, more expenditure for the broadcasters, their subscribers and shareholders (many of them are the general public for listed broadcasters) and more inconvenience for the lawful subscribers*
 - ◆ *Overseas experiences have confirmed that mere technological measure is not sufficient. There must be a parallel legal deterrent*
- **Targeting fraudulent reception for commercial purposes only is inadequate**
 - ◆ *It cannot alleviate the problem as most unauthorised decoders are used for private and domestic purposes*
 - ◆ *There is no logic to differentiate a theft for commercial purposes from a theft for personal gains*
 - ◆ *All the 12 overseas jurisdictions sanction pirated viewing for private purposes*
- **Whatever means they deploy and whether they do so for private or commercial purposes, those who steal signals are knowing swindlers and should be guilty of a crime as well as liable for a civil wrong**
- **The Hong Kong Government should work closely with the Mainland authorities on combating the supply of illicit devices**



SUBMISSION BY HONG KONG CABLE TELEVISION LIMITED ON REVIEW OF CERTAIN PROVISIONS OF THE COPYRIGHT ORDINANCE

Hong Kong Cable Television Limited (HK Cable) welcomes the invitation from the Commerce and Industry Panel of the Legislative Council to present its views on the captioned consultation paper. We shall concentrate on Chapter 6 “Unauthorised Reception of Subscription Television Programmes”

Unauthorised Reception of Subscription Television Programmes

1. What is pirated viewing?

- 1.1. Programme signals are the very valuable property of Pay TV stations. All Pay TV stations restrict their programme signals to authorized persons (e.g. subscribers) only. That is achieved by “locking” the signals and providing the authorized persons with a designated key (i.e. an authorised decoder) to “open” the signals.
- 1.2. In recent years, there have been more and more people using a false key (i.e. an unauthorised decoder) to break the lock and view programmes fraudulently without payment. Such misbehaviour is commonly termed “pirated viewing”.
- 1.3. As the Consultation Document has pointed out, pirated viewing has become increasingly rampant because of not only the ready availability of low-price unauthorised decoders (due to recent advances in piracy technology) but also the prolonged absence of an effective deterrent. Existing legislation deals only with supply level. Unauthorised decoders are produced and supplied by sources from across the border.

2. Pirated viewing is theft

- 2.1. Pirated viewing comprises the same elements of offence as theft namely, dishonesty, appropriation of another person’s property and an intention of permanent deprivation. In the same way that theft is punished by criminal sanctions, there is no justification to exempt the perpetrators of pirated



viewing from similar sanctions.

- 2.2. Pirated viewing is analogous to the crimes of abstraction of electricity and fraudulent use of a public telephone. The interests of the electricity and telephone companies are protected by criminal law, there is no justification to treat the interests of Pay TV companies differently.



3. End-user criminal liability is justified

3.1. It is right and proper to penalize both the suppliers and users of unauthorized decoders –

If the law were to provide that only the provider of a burglary tool has criminal liability while the burglar himself has not, nobody would agree that justice has been done. Likewise, justice has not been done if only the suppliers of unauthorised decoders, but not the users are subject to criminal liability.

3.2. Pirated viewing cannot be effectively controlled unless it is banned at the end-user level -

- a. Although the Broadcasting Ordinance has made it an offence to supply an unauthorised decoder in the course of trade or business, it has been proved to be inadequate for tackling the pirated viewing problem in Hong Kong. So far, only a handful of traders have been convicted and all of them got off with either a small fine or a social service order. Worse still, the prohibition does not apply to the Mainland which is the major source of supply of the unauthorised decoders. As a result, unauthorised decoders are still widely and openly sold in the local markets and across the border.
- b. The illicit supply will continue unless the demand is stopped. The demand will not, however, stop unless there is an effective deterrent in terms of criminal liability.

3.3. The problem is severe, it has caused and is continuing to cause significant damage –

- a. Pirated viewing is more threatening and damaging than conventional infringement of pirated videograms. A pirated videogram provides users with one or two pre-recorded programmes only. Yet, an unauthorised decoder could provide the users with all the programmes of the Pay TV station on a real time basis. The more pirated videograms a user wants, the more he needs to pay. Yet, a user of an unauthorised decoder continues to



gain unlimited access to programmes without cost until the unauthorised decoder is removed or disabled.

- b. It is estimated that there are at least 100,000 unauthorised decoders in use for reception of HK Cable programmes, compared to the authorised number of around 560,000. Local and international media and programming suppliers, whose revenues are directly or indirectly based on the subscription revenue received by HK Cable are equally affected. Additionally, the Government has also incurred financial loss in terms of tax revenue.
- c. The piracy problem has severely damaged the attractiveness of Hong Kong as a regional broadcasting hub. According to CASBAA¹, many regional broadcasters and content providers have suspended or cancelled their investment plans in Hong Kong because they perceive their property and financial interests are not adequately protected here. In the end, Hong Kong will lose not only choice of quality programming but also foreign investments.
- d. Pirated viewing is generating enormous amounts of undue profits for the manufacturers and providers of illicit devices. AEPOC² has estimated that illegal turnover in illicit devices is in the region of 1 billion Euro yearly. Without robust legislation, Hong Kong may become a haven for the suppliers of illegal decoders which would undermine the promotion of Hong Kong as a regional broadcasting hub.
- e. Unauthorised decoders do not have a parental lock. Thus, children could be easily exposed to programmes not suitable for them. Parents who use unauthorised decoders could give children a wrong message that greed and

¹ CASBAA (The Cable & Satellite Broadcasting Association of Asia) is the region's leading non-profit trade organization for the promotion of multichannel television and data transmission via cable and satellite networks. The CASBAA membership consists of leading cable and satellite system operators and programmers; suppliers and manufacturers of cable and satellite technology; related business service providers; communications, advertising & marketing executives, members of the media, government regulatory bodies, telecom companies, new media service purveyors, network enablers and individuals committed to upholding and promoting industry standards.

² AEPOC is the European Association for the Protection of Encrypted Works and Services. Its members include 21 major players in the digital television and telecommunications sectors, operating internationally.



dishonesty are acceptable.

3.4. *Implementation of the criminal law is not intrusive -*

- a. HK Cable respects civil liberties and does not approve of casual entry into premises, in particular domestic premises, by law enforcement agency. Yet, it would create a big loophole if the law enforcement agency can never enter domestic premises to combat crimes.
- b. It is possible to strike a balance by requiring the law enforcement agency to seek the court's approval (in the form of a warrant) before entering any domestic premises, with no warrant issued unless the enforcement agency can provide the magistrate with sufficient information on oath and, the court is satisfied there are reasonable grounds for suspecting that a crime has been committed in the premises or evidence of crime can be collected in the premises.
- c. HK Cable believes it is possible to provide evidence technically to show reasonable grounds for suspecting the use of an unauthorised decoder without entering the premises by confirming that no service subscription exists for the premises but there is reception of Pay TV programme signals at the premises. Bearing in mind that it is a criminal offence to provide false information on oath, neither the law enforcement agency nor the Pay TV operator is likely to make an unfounded application for a warrant.
- d. Power to enter into domestic premises with a warrant for law enforcement purposes is common in Hong Kong for both serious and mild offences. For example,
 - S.123(1) of the Copyright Ordinance provides, "A magistrate may, if he is satisfied by information on oath that there are reasonable grounds for suspecting that there is in any place any article or thing which may be seized, removed or detained under section 122(1)(b), issue a warrant authorizing an authorized officer to enter and search the place".
 - S.6 of the Broadcasting Ordinance provides, "Where a magistrate is



satisfied by information on oath that there are reasonable grounds for suspecting that there is an unauthorized decoder in any domestic premises used by a person whom he has reasonable grounds for believing has committed an offence under this section, then he may issue a warrant authorizing the Telecommunications Authority or any other public officer to enter and search the premises".

More examples could be found in other Ordinances. Foreign jurisdictions have similar requirement. These confirm that power to enter domestic premises with a warrant is a generally accepted practice for law enforcement purposes.

- e. A householder using an unauthorised decoder to gain access to Pay TV services is defrauding the Pay TV company of at least HK\$3000 per year. This is not an inconsiderable sum. If the householder were thought to have stolen a television set of a similar value, there would be no thought of not entering the premises to gain evidence for a conviction. With the safeguards outlined above, we believe it is not unreasonable for the law enforcement agency to enter domestic premises for gaining evidence for the prosecution of the users of unauthorised decoders.

3.5. *It targets only the knowing swindlers and does not jeopardize the innocent public –*

- a. The public complaints about the imposition of end-user liability in April 2001 revolved primarily around the copying and keeping of cuttings of newspapers and other publications which are necessary for the daily operation of many schools and business entities. It is, however, unlikely that such schools, business entities or anyone else would need an unauthorised decoder to receive our programmes on legitimate grounds.
- b. It is appreciated that there could be innocent infringement of VCD, CD and software copyright since the genuine and counterfeit copies of such works may sometimes be difficult to distinguish. There is however no similar difficulty for users of unauthorised decoders because they will know whether they are making subscription payments to the Pay TV stations for the programmes received. HK Cable, furthermore, has not authorized any



outside party to sell or lease its decoders.

4. End-user criminal liability is not a new idea

- 4.1. In 1993, the Law Reform Commission of Hong Kong accepted that fraudulent reception of a transmission should be a criminal offence³. The Commission specifically recommended that section 297 of the UK Copyright Designs and Patents Act 1988 (i.e. offence of fraudulently receiving programmes) be adopted in its totality. This recommendation was made after extensive and thorough discussions, researches, public consultations, debates and comparisons with the overseas laws in the six years from 1987. Unfortunately, the recommendation had not been included in the Copyright Ordinance when it was enacted in 1997.
- 4.2. HK Cable's investigations have shown that at least 12 jurisdictions, including United Kingdom, United States, France, Canada and New Zealand, make the end users liable for gaining illicit access to encrypted television services. All of these jurisdictions provide both criminal sanctions and civil/other remedies. Appendix A summarizes the legal positions of the 12 jurisdictions. It is important to note that none of these jurisdictions has regarded such measures as contravention of human rights or civil liberties (many of these jurisdictions are well-known for having high regard for human rights and civil liberties).

5. Civil liability alone is inadequate

- 5.1. Some people have suggested that pirated viewing should be tackled by civil liability alone because they argue that enforcement of the criminal law is intrusive. HK Cable cannot see the logic why it will be more intrusive for a public officer than a HK Cable staff to knock at a suspect's door. The argument appears to be based on the unreasonable presumption that the public officers will abuse their powers and the statutory safeguards against unlawful entry into premises (mentioned in para. 3.4) are inadequate. We disagree with this view.

³ Paragraph 11.69 of the Commission's Report on Reform of the Law Relating to Copyright (Topic 22)



- 5.2. If no criminality liability existed, Pay TV companies would be at a significant disadvantage in controlling the usage of unauthorised decoders. Collecting evidence for civil proceedings can be particularly difficult. In the case of domestic premises for example, the caretakers may expel our investigators at the entrance of the buildings. Public places such as pubs, karaokes and places of entertainment are risky for civil investigators to collect evidence without protection of law enforcers.
- 5.3. Civil liability has no deterrent effect. Most users of unauthorized decoders believe that the probability of being sued is low because the number of such users is large. Even if caught, the consequence will be minor with nothing more serious than payment of the outstanding subscription fees.
- 5.4. Civil liability should only serve as a supplement by providing the Pay TV companies with an opportunity to recover their losses.

6. Technological measure alone is inadequate

- 6.1. HK Cable has been investing several hundred million dollars in upgrading its encryption system, including a complete digitization of the system. Nevertheless, the adoption of digital encryption system will only be able to buy time, as there is no security system which is absolutely secure. There have been reports that the digital encryption systems deployed by certain broadcasters in Europe and United States have been broken⁴. The broadcasters are forced to play cat-and-mouse game with illegal suppliers. The more frequent the modifications, the more business opportunities for the suppliers of illegal equipment, the more expenditure for the broadcasters, their subscribers and shareholders (many of whom are members of the general public for listed broadcasters) and the more inconvenience to the lawful subscribers. In the end, every party other than the manufactures and sellers of the illicit devices is loser.

⁴ See, for example, "Cracking down on the digital pirates" (22 Feb. 2001) on www.guardian.co.uk which describes the sale of pirate ONdigital cards in Scotland; "DIRECTV seizes signal theft equipment from businesses nationwide" (27 Jun. 2001) on www.directv.com/press and "ITV Digital falls prey to smartcard piracy" (19 Sept. 2001) on news.zdnet.co.uk



6.2. There has been a suggestion that the pirated viewing problem can be tackled if HK Cable disconnects all drop cables (i.e. the wiring connecting individual home to the network of HK Cable) of non-subscribers from HK Cable's network. The suggestion does not work. By virtue of the mandatory interconnection requirement, the HK Cable's network carries, on top of its Pay TV signals, signals of other television and telecommunications companies. Thus, all these signals are transmitted via the same drop cables to individual premises. If the drop cables are disconnected, the non-subscribers will lose all such television and telecommunications services.

6.3. Elimination of pirated viewing cannot be achieved solely by technological measure. There must be a parallel legal deterrent.

7. Targeting fraudulent reception for commercial purposes only is inadequate

7.1. HK Cable estimates that around 95% of unauthorised decoders in use are installed at domestic premises. Banning use of unauthorised decoders for commercial purposes only will not target this large and growing problem. As we have argued, pirated viewing is theft. We cannot see the justification for differentiating a theft for commercial purposes from a theft for personal gains in the determination of liability.

7.2. As seen from the Appendices, twelve overseas jurisdictions have banned pirated viewing for private purposes by one way or another. For example, although the United Kingdom legislation forbids only commercial possession of unauthorised decoders, there is a back-up provision against fraudulent reception (s.297 CDPA) which could catch domestic pirates.

8. Conclusion

Pirated viewing is not merely a problem of copyright infringement. It is a crime of theft. It has caused and is continuing to cause substantial losses to the broadcasting industry, local and overseas programming partners and the Treasury of the Government. The problem is escalating. If it cannot be stopped immediately, it may dampen all the effort, time and money invested



in the development of Hong Kong as a regional broadcasting hub. Overseas experiences have confirmed that the problem cannot be effectively tackled by technological measures alone nor restraints at the supply level. It has been widely accepted around the world that imposing end-user criminal liability on pirated viewing for both private and commercial purposes is both justifiable and constitutional. Irrespective of the means they employ, those people who fraudulently receive Pay TV programmes are knowingly defrauding the Pay TV companies, they are not innocent (unknowing) copyright infringers. It is therefore appropriate to make them guilty of a crime as well as liable for a civil wrong.

In addition, we would urge the Hong Kong Government to work closely with the Mainland authorities on combating the production and sale of the illicit devices in the Mainland.

Hong Kong Cable Television Limited

January 2002



Overseas Prohibitions on Illicit Access to Encrypted TV Service

<u>Territory</u>	<u>Illegal Activities</u>	<u>Criminal Sanctions</u>	<u>Civil / Other Remedies</u>	<u>Legislation</u>	<u>Purposes of the Illegal Activities</u>
United Kingdom	Dishonestly receiving a TV / radio programme with intent to avoid payment	Fine	-	S.297 Copyright Designs and Patents Act 1988	Private and/or commercial
	Possessing or installing an unauthorised decoder	Imprisonment (up to 2 years) and/or fine	Delivery up, seizure, injunction, damages, recovery of costs etc.	S.297A & 298 Copyright Designs and Patents Act 1998	Commercial
United States	Intercepting or receiving any communication service offered over a cable system without authorization	Imprisonment and / or fine	Injunctions, damages and recovery of full costs	S.633 Communications Act 1934 (as amended by the Telecommunications Act 1996)	Private and/or commercial
	Intercepting radio communication, receiving interstate or foreign communication by radio and using such information for personal or other benefits without authorization.	(more severe penalty if the violation is for commercial advantage or private financial gain)		S.705 Communications Act (as amended by the Telecommunications Act 1996)	Private and/or commercial
	Circumventing a technological measure that effectively controls access to a copyright protected work	Imprisonment and/or fine	Injunctions, damages and recovery of costs, etc.	S.1201(a), 1203 & 1204 Digital Millennium Copyright Act 1998	Private and/or commercial



Canada	Decoding an encrypted subscription programming signal or encrypted network feed without authorization	Imprisonment and / or fine	Damages, injunction, accounting and other appropriate remedies	S.9, 10, 18 Radiocommunication Act	Private and/or commercial
	Operating a radio apparatus so as to receive an encrypted subscription programming signal or encrypted network feed that has been decrypted without authorization				
	Importing or possessing any equipment or device for decoding the said encrypted signal / feed without authorization				
	Fraudulently, maliciously or without colour of right obtains any telecommunication service (which, by definition, includes TV programme and Internet services)	Imprisonment	Forfeiture of the device	S.326, 327 Criminal Code	Private and/or commercial
Possessing any device to obtain telecommunication service (which, by definition includes TV programme and Internet services) without payment					
Finland	Unlawful possession, use and import of a decoding system for a protective code.	Fine	Confiscation of such decoding system, seizure of economic benefit derived from the commission of the	S.25, 42, 45 ,46 Telecommunications Market Act	Private and/or commercial



			crime		
Ireland	Intercepting any protected service, possessing, importing or installing any equipment for the purpose of enabling such interception ("Intercepting" means receiving, viewing, listening to, recording by any means of a broadcasting service without the agreement of the service provider)	Imprisonment and / or fine (up to 3 months or £1000 on summary conviction up to 2 years & £20,000 on conviction on indictment)	Forfeiture of such equipment, injunction, damages and / or an account of profits	S.9, 10, 11, 12, 15 Broadcasting Act 1990	Private and/or commercial
Iceland	Using decoder to receive an encoded broadcast without payment of subscription fee	Imprisonment and / or fine	Confiscation of any objects and equipment that were used to commit the infringements and profits derived from such infringements	Article 28, 29, 33 Broadcasting Act	Private and/or commercial
New Zealand	Receiving a TV / radio programme with intent to avoid payment	Fine	Order for delivery up	S.227, 228 Copyright Act 1994	Private and/or commercial
Fiji	Receiving a TV / radio programme with intent to avoid payment	Fine	Order for delivery up	S.224, 225 Copyright Act 1999	Private and/or commercial
*France	Private possession or acquisition (with intent to use) of equipment, appliances or instruments designed wholly or partly to fraudulently receive protected broadcast programmes	Imprisonment (up to 2 years) and / or fine (up to Euro 30490)	Confiscation of such equipment, appliances, instruments and relating advertising material	Article 79, French Audiovisual Law (Loi No. 86-1067)	Private



*Belgium	<p>Unauthorized reception of pay-TV service</p> <p>Receiving a decrypted programme from a third party without authorization</p> <p>-----</p> <p>Importing, possessing, installing, purchasing or renting unauthorised decoding device</p>	<p>Fine (up to Euro 248)</p>	<p>Confiscation of any devices that were used to commit the offence</p>	<p>Article 19, 43 Decret of 27 July 1987 on broadcasting</p> <p>-----</p> <p>Decret of 25 January 1995 on broadcasting</p>	<p>Private and/or commercial</p>
*Nether-lands	<p>Making use, by illicit decoding devices or otherwise, of a service which is offered to the public by way of telecommunications (including TV service), with intent not to pay the full price</p>	<p>Imprisonment (up to 3 years) and / or fine (up to Euro 45378)</p> <p>(More severe penalty if the offence was performed professionally)</p>	<p>Seizure of goods and profits, publication of the sentence and expulsion from the occupational field</p>	<p>Article 48, 326C Wetboek van Strafrecht (Penal Code)</p>	<p>Private and/or commercial</p>
**Italy	<p>Personal Possession of pirate equipment</p>	<p>Imprisonment (up to 3 years) and/or fine</p>	<p>Seizure etc.</p>	<p>Italian Law 248/2000</p>	<p>Private</p>

* Source: “Study on the use of conditional access systems for reasons other than the protection of remuneration, to examine the legal and the economic implications within the Internal Market and the need of introducing specific legal protection” – Report presented to the European Commission by N.Helberger, N.A.N.M. van Eijk and P.B. Hugenholtz, University of Amsterdam, April 2000.

** Source: Press Release dated 26 June 2001 of AEPOC (Association Europeenne pour la Protection des Oeuvres et Services Cryptes).