Submission by Hong Kong Cable Television Limited (CABLE TV) to the Panel on Information Technology and Broadcasting of the Legislative Council at its meeting on July 11, 2005 in respect of Domestic/private pirated viewing of subscription television programmes

Background

The Legislative Council last considered the issue of pirated domestic/private viewing of pay TV programmes, or Pay TV signal theft, at length during deliberation of the *Broadcasting (Amendment) Bill* in 2004.

Despite our strenuous submission at the time (and over the years) that the problem of pirated viewing cannot be stamped out without criminal sanction against the domestic end-user, the Administration had refused to make pirated domestic/private viewing a criminal offence when the *Bill* was passed into law.

Instead, the Administration had maintained that the problem "has stemmed largely from CABLE TV's analogue transmission" and only agreed to introduce criminal liability on domestic end-users "if domestic pirated viewing remains rampant after completion of digitalisation by HKCTV."

We wish to report to the Panel that CABLE TV's digitalisation has been completed towards the end of 2004, months ahead of the May 2005 schedule.

Taking advantage of digitalisation and the latest security measures pertaining thereto, CABLE TV has been further and constantly upgrading its transmission security system. The latest technologies have been applied; the security and version of smartcards are updated, digital security codes are changed frequently – up to many times a day recently (see Annex 1).

Regrettably, we wish to inform Member that despite our continuing best effort, made at considerable costs and manpower, to maintain a robust security system, and despite repeated enforcement action by the authorities on the trading of illegal decoding devices after ditigalisation has completed, the problem of pirated domestic/private viewing of Pay TV remains rampant.

Current state of the problem

We have been continuing with our regular inspections of illegal decoder trading hotspots. Our inspections showed that illegal vendors are active as ever. This is despite repeated raids by law enforcement officers.

Following full digitalisation of Cable TV broadcast, the formerly popular analogue decoding devices have disappeared. However, a new generation of decoding devices designed to hack into our digital service has emerged.

We observed the following main types of hacking devices/methods currently in use to circumvent our digital security system:

1.Auto-roll Receiver - designed to circumvent all Cable TV digital security key code changes *automatically*.

2.Receiver with programmable smartcard – designed to circumvent Cable TV digital security key code changes, manually by user using re-programming device (抄咭器)with codes supplied by vendor through pager message and/or website.

3.Modified Cable TV set-top box smartcard – legitimate Cable TV smartcards are modified to enable subscribers of low-cost plans with limited number of viewable channels to access all 90-plus Cable TV channels.

The trend

Most worrying is the trend of increasing sophistication of the illegal vendors, both in terms of the technology they are using, and the way they are operating despite CABLE TV's incessant efforts to introduce counter-measures. (See Annex 1)

The selling price of illegal devices is also dropping sharply, thereby increasing the attraction to illegal viewers.

Modus operandi

Apart from selling illegal devices, vendors also provide "after-sale" service by setting up special websites and pager contact points to provide new security digital key codes to users on an on-going basis.

An example is the website: www.fydvb.com, on which key codes are posted on a roving basis. The site also offers illegal decoders for sale.

We also have other reasons to believe that the vendors are operating in a highly-organised syndicated fashion with sophisticated operatives.

Technology

The programmable smartcard and the latest auto-roll devices are both designed specifically to bypass our digital security system. The auto-roll device is the latest "users' choice" as it purports to eliminate even the need to change the key code.

In the middle of June 2005, our undercover investigators purchased the latest auto-roll smartcard from an illegal vendor in Ap Liu Street at $600. The smartcard was promoted as "Everlasting Card" (不死咭) that is purported to be "immune" to our security key code changes.

Lowering prices of illegal devices

The selling prices of illegal decoding devices are on a consistently downward trend. The trend has been the same both in the pre-and-post analogue phases. Towards the end of the analogue era about two years ago, illegal decoders were available for as low as $230.

After we have switched to digital, re-programmable smartcards designed to crack the system were initially sold for more than $1,000. It has since dropped to as low as $350 or lower. The price for the card re-programming device, meanwhile, has dropped from $250 to $200.

The lower the selling price of the various illegal decoding devices, the more attractive they are to the end-users vis-a-vis the recurrent monthly subscription fee, thus aggravating the problem.

Response to the Administration's latest position

We noted the Administration position, as set out in its paper to this Panel CB(1)1985/04-05(04), that it is maintaining its position of not introducing criminal

sanction against domestic/private Pay TV service pirates.

We are, however, unable to agree with the arguments the Administration has proffered therein in support of its latest position, which, in our respectful view, are wholly untenable.

The Administration argued, in *Paragraph 15*, that "For individual pirated viewing for domestic purposes, taking into account the degree of harm, enforcement considerations, and the fact that digitalisation has contained the problem, civil remedies are the appropriate legislative measure."

On digitalisation, the Administration noted that "the selling of unauthorised decoders at blackspots has decreased substantially since HKCTV's digital migration" and drew the conclusion that "This is a good indicator that the problem of pay television piracy has reduced to a large extent." *(Paragraph 7)*

Reality is that far from having been "reduced to a large extent", the problem of piracy is serious as ever. Vendors of illegal decoding devices remain active after digitalisation, as is observed by our investigators (the latest inspection on July 3, 2005).

The Administration's observation has failed to take into account that reduction in illegal vending activities, if any, may be due to a number of factors, one of which is the chilling effect following raids by law enforcer. Such "hibernations" are often short term as is shown by past experience.

The Administration has also failed to take into account that, making use of the advancement in technology, illegal traders are shifting their trading ground to platforms such as the Internet. Their activities have not reduced, they have just become more sophisticated, more high-tech, hence invisible and harder to detect. Information we set out in the earlier part of this submission are clear indication that digitalisation has not, and will not, solve the problem.

It is noted, in Paragraph 16(a) that "legislative sanction would need to be proportional to the harm caused by the misdeed in question." Pay TV signal theft is no different from theft, which is a criminal offence. It is hard to understand why this kind of theft is singled out as one for civil remedy alone. The harm done is hardly relevant where the act in question is criminal in nature. Where else in our law is the extent of "harm

done" a factor for relieving criminal liability for the offence of theft? It is as irrelevant as arguing that someone who stole a bar of candy from a supermarket should just be subject to civil liability.

In any event, the harm of Pay TV signal theft is more than substantial to justify criminal sanction. One estimate (CASBAA) has put the cost of pay-TV signal theft in Hong Kong in 2004 at HK$194 million (US$ 24.9 million). The argument of proportionality is simply not relevant on this question.

Just as irrelevant is the argument about "enforcement consideration", namely, that "it is practically difficult to detect the use of unauthorised decoders outside the relevant domestic premises, it would not be easy to identify the target for enforcement." *(Paragraph 16(a)).*

If this line of argument is valid, most criminal offences in our statute books will have to be deleted. This argument also shows up the unreasonableness in asking individual Pay TV operators to enforce the law by taking civil remedy. If the Government, with the full support of its powerful enforcement machineries, finds it "practically difficult" to tackle offenders, what chance would private enterprises have in successfully doing so?

End-user criminal sanction is needed

It is clear that the illicit trade of illegal decoders to domestic end-users remains rampant despite our best effort in upgrading security after full digitalisation. There are, in fact, also signs that the situation is deteriorating with the illegal vendors becoming more sophisticated.

Obviously, present legislation, which exempts the private/domestic end-users from criminal liability, is inadequate in controlling the problem. Nor would digitalisation alone, as we have pointed out to the Administration in the past repeatedly.

The reasons are equally obvious. No matter how diligent Pay TV operators are in upgrading and updating their system security, and no matter how fast operators apply the latest technology, illegal traders will find a way to catch up. Technology is a double-edge sword, accessible to the legal and illegal operators alike. So long as there are subscription fees to avoid, there will always be a demand for illegal decoding devices, and in turn, a market for illegal traders to exploit. The cat-and-mouse game

will never end unless end-users are effectively deterred. This means imposing the appropriate sanction, which is criminal liability, for the illegal act – of stealing a pay service - is unmitigated theft.

Yet the Administration has been unwilling to impose criminal sanction on end-users, and this is baffling. The Administration's tolerance to this one group of domestic pirates is in stark contrast to the overall government effort in combating intellectual property rights infringements, such as the recent high profile clampdown on BT piracy. It begs the question why the Administration considers some sector of the creative industry more worthy of protection than others.

The Government's persistent refusal to impose criminal sanction on domestic Pay TV service pirates also runs against the worldwide trend in dealing strictly and urgently with the grave problem of intellectual property piracy, which is threatening to get out of hand as pirates make use of rapid advancements in technology. More jurisdictions have introduced or are in the process of introducing criminal sanction against pirated viewing at home. One of the latest countries to criminalise private pirated viewing is Singapore, which has made this an offence under its Broadcasting Act; similar law is going through the legislating process in Australia.

Summing up

We see no further reason to further put off the criminalisation of domestic/private piracy of Pay TV service in Hong Kong, which is the main part of the Pay TV privacy problem.

Therefore, we request the Panel to urge the Administration to proceed forthwith to introduce legislation imposing end-user criminal liability on pirated domestic/private Pay TV viewing.

- End-

Domestic/Private pirated viewing of subscription TV programmes Situation Update

Presentation by

Hong Kong Cable Television Ltd.

to

Panel on Information Technology and Broadcasting

July 11, 2005

有線電視 CABLE TV

Digitalisation completed with enhanced security measures

- CABLE TV digitalisation completed by end of 2004 ahead of schedule
- Robust new security counter-measures for digital broadcast implemented vigorously

有線電視 CABLE TV

Digitalisation completed with enhanced security measures

- Major counter-measures, including key changes and smartcard security/version upgrading – no less than 14 times throughout 2004, and 2005 so far

- Daily key changes – up to 6 times daily – implemented

有線電視 CABLE TV

Piracy problem remains rampant

- Despite efforts by CABLE TV to enhance, upgrade, update security system, domestic/private pirated viewing problem remains rampant after digitalisation

有線電視 CABLE TV

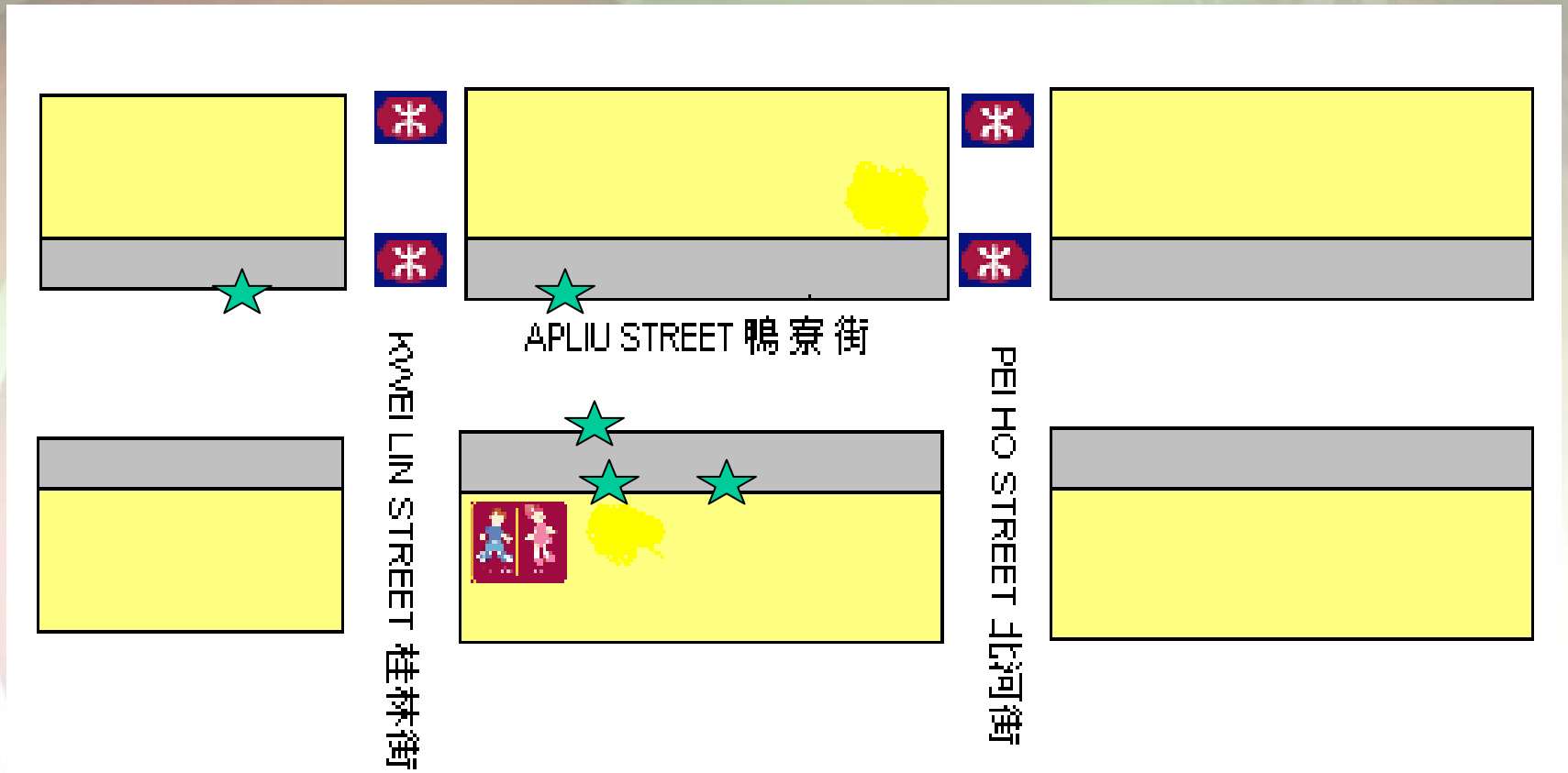
State of the problem

- Illegal decoding devices vending remains active at blackspots like Ap Liu St.

- New generation hacking devices emerge to circumvent Cable TV’s new digital broadcast system security

有線電視 CABLE TV

Locations of illegal decoder vendors
July 2005



有線電視 CABLE TV

Main types of current hacking devices/methods

- **(1) Auto roll receiver**

  Designed to circumvent frequent CABLE TV digital security key changes automatically

  (*Purported to be valid for 6 months*)

有線電視 CABLE TV

Main types of current hacking devices/methods

- **(2) Receiver with programmable smartcard**

  Designed to circumvent frequent CABLE TV digital security key changes manually using re-programming device (抄咭器)

  (codes supplied via website/ pager message)

有線電視 CABLE TV

Card writer –
for receiver with programmable smartcard

有線電視 CABLE TV

Main types of current hacking devices/methods

- **(3) Modified Cable TV smartcard**

  Converting smartcards for low-cost subscription package to access all 90+ CABLE TV channels

有線電視 CABLE TV

The worrying trend

- **Sophistication**

  Illegal vendors becoming more sophisticated – in technology and in the way of operation

- **Falling prices**

  Selling prices of illegal decoding devices keep declining – becoming more and more attractive to illegal viewers

有線電視 CABLE TV

The worrying trend

- **After-sale service**

  Syndicated mode of operation, with website and pager message system supplying digital security code to users on ongoing basis

- **Technology**

  Latest auto-roll device with “Everlasting Card” (不死咭) purportedly “immune” to CABLE TV digital security measures

有線電視 CABLE TV

The worrying trend

Declining prices

Analogue devices -

- $230 at final stage

Digital devices – (dropped within months)

- Smartcards from $1,000 to $350
- Card writer from $250 to $200

有線電視 CABLE TV

Response to latest Govt position

Govt arguments wholly untenable…

- Digitalisation has not “reduced to a large extent” the problem of Pay TV signal theft
- Proportionality argument not relevant
- Why is theft not criminal?

有線電視 CABLE TV

Response to latest Govt position

Govt arguments wholly untenable…

- No harm? CASBAA puts costs of Pay TV signal theft to Hong Kong in 2004 at HK$194 million

- Enforcement “practically difficult”? Is it then reasonable to expect private enterprise to enforce by civil action?

有線電視 CABLE TV

End-user criminal sanction needed

- Piracy remains rampant after full digitalisation
- Clear signs of situation deteriorating
- Present legislation unable to control problem
- Contrast with overall Govt stance on IP protection
- Runs against worldwide trend
- Discriminatory treatment of Pay TV sector

有線電視 CABLE TV

End-user criminal sanction needed

- As Hong Kong dragged its feet, more jurisdictions have introduced end-user criminal sanction – e.g. Singapore and Australia

- **No more reason for Hong Kong to further delay imposing criminal sanctions on domestic/private Pay-TV pirates**

有線電視 CABLE TV

Thank you

有線電視 CABLE TV