LC Paper No. CB(2)2193/02-03(01)

Legislative Council Subcommittee on the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002

Purpose

This note provides further information on the issues raised in relation to the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2) Order) 2002 (the draft Order) at the meeting of the Subcommittee on 17 March 2003.

Mutual legal assistance and extradition of offenders

2. Double criminality is a prerequisite under Hong Kong law for international cooperation in respect of mutual legal assistance and surrender of fugitive offenders. This is stated in section 5(1)(g) of the Mutual Legal Assistance in Criminal Matters Ordinance (Cap. 525) and section 2(2) of the Fugitive Offenders Ordinance (Cap. 503) -

Section 5(1)(g) of Cap. 525

"A request by a place outside Hong Kong for assistance under this Ordinance shall be refused if, in the opinion of the Secretary for Justice –

the request relates to an act or omission that, if it had occurred in Hong Kong, would not have constituted a Hong Kong offence."

Section 2(2) of Cap. 503

"For the purposes of this Ordinance, an offence by a person against the law of a prescribed place is a relevant offence against that law if -

(a) the offence is punishable under that law with imprisonment for more than 12 months, or any greater punishment; and

(b) the acts or omissions constituting the conduct in respect of which the person's surrender to that place is sought amount to conduct which, if the conduct had occurred in Hong Kong, would constitute an offence –

(i) coming within any of the descriptions specified in Schedule 1; and

(ii) punishable in Hong Kong with imprisonment for more than 12 months, or any greater punishment."

3. As we have explained in an earlier paper (LC Paper No. CB(2)1324/02-03(01)) submitted to the Subcommittee, traditional jurisdictional rules forbid Hong Kong to exercise jurisdiction over the three computer offences[1] covered by the draft Order, if the perpetrators who obtain access to the computers or the computers to which access is obtained are outside Hong Kong. In other words, such unacceptable acts at present do not constitute offences in Hong Kong. Under the principle of double criminality, the existing arrangements on mutual legal assistance and surrender of fugitive offenders would not be applicable to these acts.

Mutual legal assistance

4. With the enactment of the draft Order, Hong Kong will be able to make a request to other jurisdictions for mutual legal assistance (and obtain assistance) in respect of the three computer offences, if the alleged criminal conduct is also considered as constituting an offence in the requested jurisdiction under its relevant laws.

---

[1] The three computer offences are -

(a) "unauthorized access to computer by telecommunications" under section 27A of the Telecommunications Ordinance (Cap. 106);

(b) "destroying or damaging property" relating to the misuse of a computer under sections 59 and 60 of the Crimes Ordinance (Cap. 200); and

(c) "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance (Cap. 200).

5. With the same token, a request from an overseas jurisdiction for assistance involving the three computer offences may be processed under the relevant mutual legal assistance agreement with that jurisdiction, or on an ad hoc basis under the Mutual Legal Assistance in Criminal Matters Ordinance.

Surrender of fugitive offenders

6. Upon the enactment of the draft Order, if computer offences are on the list of extraditable offences specified in an agreement on surrender of fugitive offenders, Hong Kong will be able to seek the surrender of fugitive offenders for the two offences of "destroying and damaging property" relating to the misuse of a computer and "access to computer with criminal and dishonest intent" under the Crimes Ordinance[2].

7. Similarly, Hong Kong may surrender offenders in respect of the two computer offences committed in the requesting jurisdiction.

The case on the "Love Bug" computer virus

8. The case was about the spreading of the "Love Bug" computer virus in May 2000, which was usually known as the "I love you" virus or technically referred to as "VBS.LoveLetter". The virus was first reported to originate from the Philippines. It was estimated that at least 600,000 computers had been infected, affecting some 45 million people worldwide.

9. The Filipino authorities had identified four suspects in the Philippines. However, prosecutions were eventually dropped or dismissed, as there were then no computer crime laws or other appropriate legislation in the Philippines based on which the charges could be substantiated. We understand that no extradition had been effected in respect of the case.

---

[2] The offence of "unauthorized access to computer by telecommunications" under the Telecommunications Ordinance (Cap. 106) is not covered by the surrender of fugitive offenders regime, as it attracts a maximum penalty of only a fine of $20,000.

Elements of the offence under section 161 of the Crimes Ordinance

10. Section 161[3] of the Crimes Ordinance (Cap. 200) was enacted in 1993 by the Computer Crimes Ordinance [4], based on the recommendations in the report of 1988 of the Attorney General's Chambers Working Group on Computer-related Crime (the Working Group).

11. The Working Group had observed that under the then existing law, most of the preparatory work for computer-related crime could be performed without committing any offence. It was considered desirable that unequivocal preparatory work which consisted of gaining access to a computer dishonestly and with intent to deceive or to cause loss to another or gain for the wrongdoer should be specifically punishable without waiting for the plan to be carried to completion or for it to amount to an attempt to carry out those offences. The Working Group therefore recommended creating a new computer offence of "dishonest accessing" along the lines that "any person who dishonestly accesses a computer, whether with or without due authority, with intent to deceive or with a view to gain for himself or another or with intent to cause loss to another, shall be guilty of an offence and shall be liable on conviction upon indictment to imprisonment for 5 years."

---

[3] Section 161 of the Crimes Ordinance states that "any person who obtains access to a computer -

(a) with intent to commit an offence;

(b) with a dishonest intent to deceive;

(c) with a view to dishonest gain for himself or another; or

(d) with a dishonest intent to cause loss to another,

whether on the same occasion as he obtains such access or on any future occasion, commits an offence.".

[4] The Computer Crimes Ordinance has, through amending the Telecommunications Ordinance (Cap. 106), the Crimes Ordinance (Cap. 200) and the Theft Ordinance (Cap. 210), created some new computer offences and broadened the coverage of existing offences to cater for circumstances involving the use of computers.

12. Indeed section 161 of the Crimes Ordinance was considered in detail by the Court of First Instance in the case of HKSAR v Tsun Shui Lun [1999] HKCFI 62. The then Chief Judge of the High Court (CJHC) considered that a section 161 offence required proof of a specific criminal or dishonest intent or purpose and was more serious than the offence under section 27A (unauthorized access to computer by telecommunications) of the Telecommunications Ordinance. The *actus reus* of the offence is obtaining access to a computer. Each of the four situations under section 161(1) constitutes the *mens rea* of the respective crime. Section 161 is intended to criminalize access to a computer with a particular intent or for a particular purpose. The intent with which or the purpose for which the access is made must be either criminal or dishonest.

13. In his judgement CJHC referred to the submission of the appellant's leading counsel that the legislative intent of section 161, as stated by the then Secretary for Security in his speech in the Legislative Council on the resumption of Second Reading of the Computer Crimes Bill, was to create an offence aimed at penalizing access to a computer for acts preparatory which fell short of the commission of a crime or a fraud. In rejecting the submission, CJHC stated -

> "It is clear from the section that it catches acts preparatory to the commission of a crime or fraud. But I do not agree that it is restricted to such acts. A person who makes an unauthorized access into another person's computer need not have any intention to commit a crime or fraud. He may be a businessman who wants to acquire information about his competitors in order to enable himself to have an advantage over them. He may be a disgruntled employee who wants to ruin his employer's business by revealing his employer's trade secrets to others. He may be an ex-employee who wants to obtain a list of his former employer's customers in order to solicit business from them. He may be a dissatisfied bank officer who wants to erase the bank's records from the computer in order to cause confusion or to irritate the bank's customers. All these acts may result in a gain to the perpetrator or cause huge losses, great embarrassment and serious harm to others. But they are not necessarily

criminal or fraudulent. The perpetrator's access to the computer cannot therefore be regarded as an act preparatory to the commission of a crime or fraud. However, if such access is obtained dishonestly, the perpetrator ought to be punished. That in my view is the objective of section 161(1)(c) and (d). I should think that the Secretary for Security when he was addressing the Legislative Council in 1993 was only making a generalized statement in order to summarize what the section was aimed at doing."

14. Queries were raised whether section 161 of the Crimes Ordinance criminalizes "mere intent", and whether it would be justifiable. It is noted that there are other areas of the criminal law where deception, together with another element, is regarded as sufficient to warrant the sanctions of the criminal justice system.

15. The Theft Ordinance (Cap. 210) has a variety of deception offences whereby anyone who obtains (various acts or property) by deception commits an offence if his intention is dishonest. All of the Theft Ordinance offences have four main elements -

(a) dishonesty;
(b) obtaining;
(c) property (or an act or credit or service); and
(d) deception.

Equally a section 161 offence also has four main elements -

(a) dishonesty;
(b) access;
(c) computer; and
(d) view to deceive/gain/loss.

It should be underlined that the controlling element is "dishonest". If the individual does not act dishonestly there is no offence. And dishonesty has an objective and subjective test as established in the case of R v Ghosh (1982)[5], i.e. it must be dishonest -

[5] In that case, Lord Lane Chief Justice said "In determining whether the prosecution

(a) according to the ordinary standards of reasonable and honest people; and

(b) the defendant himself must have realized that what he was doing was by those standards dishonest.

This twin test can ensure no injustice is done.

16. With the advancement of technology and the prevalence and importance of the use of computers, section 161 is legally justifiable and required in the public interest for combatting acts of access to computers which are preliminary to commission of further offences, causing loss to another or making gain by the offenders. It has been operating well since its enactment and there has not been any reported cases of miscarriage of justice in respect of this section. In any event, the prosecution has to bear the burden of proof for the offences concerned.

Whether the offences under section 161 of the Crimes Ordinance feature in the United Kingdom (UK) Computer Misuse Act 1990

17. The offence under section 161 of the Crimes Ordinance is similar to that under section 2 of the UK Computer Misuse Act 1990.

---

has proved that the defendant was acting dishonestly, a jury must first of all decide whether according to the ordinary standards of reasonable and honest people what was done was dishonest. If it was not dishonest by those standards, that is the end of the matter and the prosecution fails. If it was dishonest by those standards, then the jury must consider whether the defendant himself must have realized that what he was doing was by those standards dishonest. In most cases, where actions are obviously dishonest by ordinary standards, there will be no doubt about it. It will be obvious that the defendant himself knew that he was acting dishonestly. It is dishonest for a defendant to act in a way which he knows ordinary people consider to be dishonest, even if he asserts or genuinely believes that he is morally justified in acting as he did. For example, Robin Hood or those advent anti-vivisectionists who remove animals from vivisection laboratories are acting dishonestly, even though they may consider themselves to be morally justified in doing what they do, because they know that ordinary people would consider these actions to be dishonest."

Whether the relevant principal ordinances should be amended to set out the extra-territorial scope of the three specific computer offences

18. The Criminal Jurisdiction Ordinance (Cap. 461) was enacted in 1994 to deal primarily with international fraud, enabling Hong Kong courts to exercise jurisdiction over offences of fraud and dishonesty -

(a) Hong Kong courts will have jurisdiction if any of the conduct (including an omission) or part of the results that are required to be proved for conviction of the offences takes place in Hong Kong;

(b) An attempt to commit the offences in Hong Kong is triable in Hong Kong whether or not the attempt was made in Hong Kong or elsewhere and irrespective of whether it had an effect in Hong Kong;

(c) An attempt or incitement in Hong Kong to commit the offences elsewhere is triable in Hong Kong;

(d) A conspiracy to commit in Hong Kong the offences is triable in Hong Kong wherever the conspiracy is formed and whether or not anything is done in Hong Kong to further or advance the conspiracy; or

(e) A conspiracy in Hong Kong to do elsewhere that which if done in Hong Kong would constitute the offences is triable in Hong Kong provided that the intended conduct was an offence in the jurisdiction where the object was intended to be carried out.

In simple words, if a person in Hong Kong perpetrates a crime outside Hong Kong, or if a person outside Hong Kong perpetrates a crime in Hong Kong, that person is triable in Hong Kong courts.

19. We consider the above circumstances equally applicable to the three computer offences in question. Covering the three offences under the Criminal Jurisdiction Ordinance is therefore legally appropriate. The requirement under section 2(5) of the Ordinance that the draft Order

shall be laid before and approved by the Legislative Council ensures that the Administration's proposal is subject to a high degree of scrutiny by the legislature.

Whether any offences have been added to the UK Criminal Justice Act 1993 as far as the part on jurisdiction is concerned

20. We understand that the following offences have been added under section 1(2) of the UK Criminal Justice Act 1993, the effect being that these offences will be triable in the UK even if they involve transactions and events having taken place in more than one jurisdiction -

Added by the Theft (Amendment) Act 1996

(a) obtaining a money transfer by deception (section 15A of the Theft Act 1968);

(b) retaining credits from dishonest sources, etc (section 24A of the Theft Act 1968);

Added by the Criminal Justice Act 1993 (Extension of Group A Offences) Order 2000

(c) offences of counterfeiting notes and coins (section 14 of the Forgery and Counterfeiting Act 1981);

(d) offences of passing etc counterfeit notes and coins (section 15 of the Forgery and Counterfeiting Act 1981);

(e) offences involving the custody or control of counterfeit notes and coins (section 16 of the Forgery and Counterfeiting Act 1981);

(f) offences involving the making or custody or control of counterfeiting materials and implements (section 17 of the Forgery and Counterfeiting Act 1981);

(g) prohibition of importation of counterfeit notes and coins (section 20 of the Forgery and Counterfeiting Act 1981); and

(h) prohibition of exportation of counterfeit notes and coins (section 21 of the Forgery and Counterfeiting Act 1981).

Whether consideration of the draft Order should be deferred until completion of the scrutiny of the National Security (Legislative Provisions) Bill

21. We defer to the Subcommittee whether it would require more time to consider the draft Order, notwithstanding concurrent scrutiny of the National Security (Legislative Provisions) Bill by the Legislative Council Bills Committee.

Security Bureau
May 2003