

**立法會**  
**Legislative Council**

LC Paper No. CB(2)823/02-03(03)

Ref : CB2/SS/3/02

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

**Background brief prepared by the Legislative Council Secretariat**

**Report of the Inter-departmental Working Group  
on Computer Related Crime**

**Purpose**

This paper gives a summary of issues and concerns raised by Members on the report of the Inter-departmental Working Group on Computer Related Crime (the Working Group).

**The Working Group's recommendations**

2. At its meeting on 7 December 2000, the Panel on Security was consulted on the report of the Working Group and its recommendations. The Working Group has recommended, inter alia, that the following offences, as modified to take into account the recommendations in the report, should be covered by the Criminal Jurisdiction Ordinance (Cap. 461) -

- (a) unauthorised access to computer by telecommunications under section 27A of the Telecommunications Ordinance (Cap. 106); and
- (b) access to computer with a criminal or dishonest intent under section 161 of the Crimes Ordinance (Cap. 200).

**Issues and concerns raised by Members**

3. At the meeting on 7 December 2000, Members raised a number of issues and concerns relating to the Working Group's report. These included -

- (a) whether the existing legislation was adequate to deal with the problems of copyright infringement, illegal gambling and pornographic materials on the Internet;
- (b) the jurisdictional problem in removing offending materials on websites;
- (c) whether there were international organisations promoting the adoption of common standards and goals in combating computer-related crime;
- (d) whether there was in place a mechanism to protect critical infrastructures against cyber attacks; and
- (e) whether it was proper to make it compulsory for a person to disclose decryption tools or decrypted text.

4. The Administration had not mentioned the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 at the meeting and there were no comments from Members directly related to the addition of offences to the Ordinance.

5. The Panel met with 12 organisations/individuals at its meeting on 10 February 2001. These organisations/individuals were in general supportive of the direction in dealing with computer-related crime. They had put forward various views and suggestions on the technical aspects of the Working Group's report and related policy aspects. However, the discussions were not specific on the draft Order.

6. Members may wish to refer to the extracts from the minutes of the Panel meetings on 7 December 2000 and 10 February 2001 in **Appendices I and II** respectively for details of the discussions.

### **Way forward in respect of the Working Group's recommendations**

7. The Administration issued a Legislative Council (LegCo) Brief on the way forward in respect of the Working Group's recommendations on 16 July 2001. The Panel on Security has not discussed the way forward. The LegCo Brief is in **Appendix III** for members' ease of reference.

**EXTRACT**

**立法會**  
***Legislative Council***

LC Paper No. CB(2) 682/00-01  
(These minutes have been seen by  
the Administration)

Ref : CB2/PL/SE/1

**LegCo Panel on Security**

**Minutes of meeting**  
**held on Thursday, 7 December 2000 at 2:30 pm**  
**in Conference Room A of the Legislative Council Building**

**Members present** : Hon LAU Kong-wah (Chairman)  
Hon James TO Kun-sun (Deputy Chairman)  
Hon Margaret NG  
Hon Mrs Selina CHOW LIANG Shuk-ye, JP  
Hon CHEUNG Man-kwong  
Hon Andrew WONG Wang-fat, JP  
Hon Ambrose LAU Hon-chuen, JP  
Hon IP Kwok-him, JP

**Members attending** : Hon SIN Chung-kai  
Hon Henry WU King-cheong, BBS

**Members absent** : Hon Albert HO Chun-yan  
Dr Hon LUI Ming-wah, JP  
Hon Howard YOUNG, JP  
Hon WONG Sing-chi

**Public Officers attending** : Item III  
Miss CHEUNG Siu-hing  
Deputy Secretary for Security (Special Duties)  
  
Mr LEE Ka-chiu  
Chief Assistant Secretary for Security F

Item IV

Mrs Jennie CHOK  
Deputy Secretary for Security 2

Mr David WONG  
Principal Assistant Secretary for Security B

Mr CHAN Chun-yan  
Assistant Commissioner of Correctional Services

Mr William HUI  
Civil Secretary  
Correctional Services Department

**Clerk in attendance** : Mrs Sharon TONG  
Chief Assistant Secretary (2)1

**Staff in attendance** : Mr Raymond LAM  
Senior Assistant Secretary (2)5

---

Action

**X X X X X X**

**III. Interdepartmental Working Group on Computer Related Crime : Follow up**

(Report of Interdepartmental Working Group on Computer Related Crime and LegCo Brief Ref. : SBCR 14/3231/88 Pt.14)

6. At the invitation of the Chairman, Deputy Secretary for Security (Special Duties) (DS for S(SD)) briefed Members on the Report of the Interdepartmental Working Group on Computer Related Crime (the Report).

Jurisdictional problem

7. Referring to paragraph 8.30 of the Report, Mr CHEUNG Man-kwong asked whether existing legislation was adequate for dealing with the problems of copyright infringing articles, illegal gambling and pornographic materials transmitted through the Internet. He expressed concern about the jurisdictional problem in respect of the removal of offending materials or web sites. He said that some activities which were illegal in Hong Kong, such as gambling on football matches, might not be illegal in some other countries. He asked how the problem would be addressed by the

Action

Administration.

8. DS for S(SD) said that as these offences could also be committed through other means besides the Internet, they should be dealt with under the relevant policy context by the respective policy bureaux concerned. As an example, she cited the consultation paper entitled "Protection of Youth from Obscene and Indecent Materials : 2000 Review of the Control of Obscene and Indecent Articles Ordinance(COIAO)" — COIAO was applicable to electronic publications, and 10 out of 12 prosecutions under COIAO between January 1996 and April 2000 against electronic publications had been successful. She said that the Working Group had indeed considered the possibility of amending the offences covered by the Criminal Jurisdiction Ordinance (Cap. 461) (CJO) to all offences triable on indictment. As this might also change the jurisdictional rules regarding non-computer related offences, the Working Group recommended that consideration should be given to conducting a thorough in-depth study of the subject of jurisdictional rules in general. She pointed out that the Working Group had also recommended bringing some individual computer-related offences to be covered by CJO. As regards the removal of offending materials or web sites, she said that the Working Group had suggested that reference could be made to legislation related to copyright in the United States (US) in the formulation of take-down procedures.

Approach for implementation of recommendations

9. Mr SIN Chung-kai expressed support for the Administration's study of legislative and administrative measures against computer-related crime. He considered that non-controversial recommendations of the Working Group, such as better defining the term "computer", should be implemented as soon as possible while more controversial recommendations could be further studied. DS for S(SD) said that it was the Administration's intention to implement the recommendations in phases. However, the Administration considered it more appropriate to consult the public on the Report as a whole because it outlined a framework. Depending on the feedback received during the consultation exercise, the priority for implementing the recommendations would be decided. Mr SIN suggested that the Administration should classify the recommendations as short-term, medium-term and long-term ones to facilitate studying of the recommendations of the Working Group.

Consultation period

10. Mr SIN Chung-kai considered that the consultation period of two months for the recommendations of the Working Group was too short. He suggested that it should be extended by one month to allow more time for studying the Report. Mr Henry WU shared the same view. DS for S(SD) responded that if there was a consensus among members on the consultation period, she saw no objection to extending the consultation period to three months.

Protection of critical infrastructures from cyber attacks

Action

11. On the protection of critical infrastructures from cyber attacks, Mr James TO said that paragraphs 9.15 and 9.17 of the Report reflected that the Working Group seemed to have no knowledge about the existing situation regarding the protection of infrastructures against cyber attacks. He considered that the Police, which was also represented in the Working Group, should have been following the matter closely and aware of the existing situation. He asked whether the Working Group had contacted individual organisations to understand their plans for protection of critical infrastructures against cyber attacks.

12. DS for S(SD) responded that the Working Group had not carried out an in-depth study of the security of critical infrastructures. However, informal enquiries made by the Working Group indicated that there were contingency plans for most critical infrastructures, although there was currently no mechanism for the coordination of these plans. She said that there was not even an agreed list of critical infrastructures in Hong Kong. She added that the protection of critical infrastructure was a huge task. In US, the Commission on Critical Infrastructure Protection, which had over 60 supporting staff, took 16 months to complete its report. Referring to paragraph 9.18 of the Report, she pointed out that the Working Group recommended the establishment of a standing central coordinating mechanism to protect critical infrastructures from cyber attacks.

13. In response to Mr James TO's comment that there seemed to be no recommendation in the Report for the establishment of a committee to oversee the protection of critical infrastructures, DS for S(SD) said that the Administration was inclined to tackling the issue through existing mechanisms where feasible. A possibility was to assign the task to the subcommittee or task force that the Working Group had recommended to be established under the Fight Crime Committee (FCC). The detailed arrangements would be worked out after the overall institutional framework for addressing computer-related crime had been finalized.

Computer-related commercial crime

14. Mr Henry WU said that there was a lack of reference to computer-related commercial crime in the Report. DS for S(SD) said that a breakdown of reported cases of computer crime could be found in paragraph 1.2 of the Report.

15. Mr Henry WU said that with the development of trading of securities on the Internet, the Administration should put more effort in the prevention of computer-related crime in respect of such trading.

International co-operation against computer-related crime

16. In response to Mr Henry WU's question about whether there were international organizations promoting the adoption of common standards and goals in combating computer-related crime, DS for S(SD) said that there was currently no international organization established for such a purpose. However, various organizations, such as the Council of Europe which was preparing a Draft Convention on Cyber Crime, was

Action

working in this direction. She added that the establishment of an international contact point system among the law enforcement agencies of different countries would much facilitate combating computer-related crime. In response to Mrs Selina CHOW's question about the adequacy of the existing contact point system, DS for S(SD) said that a comprehensive international contact point system was not yet in place. The Administration would seriously consider participating in such a system when it was established.

Consultation

17. Miss Margaret NG asked whether consultation had been made by the Working Group in the discussion process. She also asked whether consultation had been made in respect of the proposed compulsory disclosure of the decryption tools or decrypted text of encoded computer records, as referred to in paragraph 8(g) of the LegCo Brief. DS for S(SD) said that the Working Group had not conducted formal public consultation in its discussion process. Since the commencement of the consultation exercise in the afternoon of 1 December 2000, no submission had been received, although there were one to two comments in newspapers.

18. Mr Henry WU declared interest as the Chairman of the Eastern District FCC. He asked whether the Administration would brief district FCCs on the recommendations in the Report. DS for S(SD) responded that a briefing had been scheduled for the chairmen of district FCCs on 22 December 2000.

Compulsory disclosure of decryption tools or decrypted text

19. Miss Margaret NG questioned whether it was proper to make it compulsory for a person to disclose decryption tools or decrypted text. DS for S(SD) said that the Working Group had considered other options, for example, depositing the decryption tools or decrypted text with an independent body but noted that privacy issues might arise from such an arrangement. She stressed that the requirement would only apply to more serious offences. Judicial authorization would also be needed for compulsory disclosure. She added that in the United Kingdom, judicial authorization was not a must and the involvement in a serious offence was not required for compulsory disclosure. Miss NG considered that the issue was related to an individual's fundamental right, rather than a person's privacy.

Other issues

20. Mr SIN Chung-kai said that the term "Internet Service Providers" was too narrow. It should be amended as "On-line Service Providers", as in US. DS for S(SD) undertook to consider the suggestion.

Adm

21. Referring to paragraph 14.2 of the Report, Mr SIN Chung-kai said that while the Administration had quoted the Draft Convention on Cyber Crime issued by the Council of Europe in April 2000, it had not pointed out that a further document issued by the Council of Europe in October 2000 revealed that about 30 organizations were opposed

Action

to the Draft Convention. DS for S(SD) explained that the Report was completed in September 2000, which was before the issue of the October version of the Draft Convention. She added that a further version was released by the Council of Europe in November 2000. She stressed that the Draft Convention only served as a reference for the Working Group.

22. Mrs Selina CHOW considered it important to educate the public on the prevention of computer-related crime. She asked about the resources allocated for the prevention of computer-related crime and the adequacy of Police manpower in combating computer-related crime. DS for S(SD) said that she had no information on hand about the amount of resource allocated. Such resource was also very difficult to quantify. She acknowledged that the adequacy of manpower resource was difficult to assess in view of the rapidly changing situation regarding computer crime. Nonetheless, should there be a need for additional manpower, requests would be submitted in the normal manner. She stressed that the prevention of computer-related crime was a key recommendation of the Report.

23. In response to Mrs Selina CHOW's question about the participation of the private sector in the prevention of computer-related crime, DS for S(SD) said that there was currently no standing mechanism for such participation. She informed Members that consideration was being given to putting more effort in this respect.

24. Miss Margaret NG commented that the Report was very technical in nature. She suggested that the legal profession and relevant industries should be invited to give their views on the subject. Members agreed that a special meeting be held on 10 February 2001 from 9:00 am to 12:00 noon to receive public views on the Report. They also agreed that all other LegCo Members would be invited to the meeting.

**X X X X X X**

Legislative Council Secretariat

15 January 2001

## *Legislative Council*

LC Paper No. CB(2) 2120/00-01  
(These minutes have been seen  
by the Administration)

Ref : CB2/PL/SE/1

### **LegCo Panel on Security**

#### **Minutes of special meeting held on Saturday, 10 February 2001 at 9:00 am in the Chamber of the Legislative Council Building**

**Members present** : Hon LAU Kong-wah (Chairman)  
Hon James TO Kun-sun (Deputy Chairman)  
Hon Margaret NG  
Hon Howard YOUNG, JP  
Hon Ambrose LAU Hon-chuen, JP  
Hon IP Kwok-him, JP

**Members attending** : Hon Eric LI Ka-cheung, JP  
Hon SIN Chung-kai  
Hon Audrey EU Yuet-mee, SC, JP

**Members absent** : Hon Albert HO Chun-yan  
Dr Hon LUI Ming-wah, JP  
Hon CHEUNG Man-kwong  
Hon Mrs Selina CHOW LIANG Shuk-yee, JP  
Hon Andrew WONG Wang-fat, JP  
Hon WONG Sing-chi

**Public Officers attending** : Miss CHEUNG Siu-hing  
Deputy Secretary for Security (Special Duties)

Mr John LEE Ka-chiu  
Chief Assistant Secretary for Security

**Attendance by : The Law Society of Hong Kong**  
**Invitation**

Mr Kevin STEEL  
Member, Criminal Law & Procedure Committee

Hong Kong Internet Service Providers Association

Mr Chester SOONG  
Chairman

The Institution of Electrical and Electronics Engineers,  
Hong Kong Section (Computer Chapter)

Dr Joseph NG Kee-yin  
Chairman

Hong Kong Computer Society

Dr Louis MA  
Vice President (Membership)

Mr Bill FOK  
Director of Community Service

International Federation of the Phonographic Industry  
(Hong Kong Group)

Mr Ricky FUNG Tim-chee  
Chief Executive Officer

Hong Kong Information Technology Federation

Mr LEE Kheng-joo  
Council Member

Hong Kong Society of Accountants

Mr Michael K H CHAN  
Chairman of Information Technology Committee

Mr Peter TISMAN  
Deputy Director (Professional Practices)

Hong Kong Information Systems Audit and Control Association  
(Hong Kong Chapter)

Ms Susanna CHIU  
Vice President

Mr William GEE  
Membership Director

Hong Kong Institution of Engineers (Information Technology  
Division)

Ir Jolly WONG  
Past Chairman

Ir K C LAI  
Hon Secretary

Webmaster (Hong Kong) Association

Ms Elizabeth QUAT  
President and Co-founder

Mr Ringo LAM  
Co-founder & Past President

Information Security and Forensics Society

Mr Ricci IEONG  
Secretary

Individual

Mr Wanbil LEE

**Clerk in attendance** : Mrs Sharon TONG  
Chief Assistant Secretary (2)1

**Staff in attendance** : Mr Raymond LAM  
Senior Assistant Secretary (2)5

---

Action

**I. To receive public views on the issues raised and recommendations made in the Report of the Inter-departmental Working Group on Computer Related Crime (the Report)**

Meeting with representative of the Law Society of Hong Kong  
(LC Paper No. CB(2) 846/00-01(01))

Mr Kevin STEEL presented the views as detailed in the submission of the Law Society of Hong Kong.

Meeting with representative of the Hong Kong Internet Service Providers Association  
(LC Paper No. CB(2) 811/00-01(01))

2. Mr Chester SOONG presented the views as detailed in the submission of the Hong Kong Internet Service Providers Association (HKISPA).

Meeting with representative of the Institution of Electrical and Electronics Engineers, Hong Kong Section (Computer Chapter)  
(LC Paper No. CB(2) 828/00-01(01))

3. Dr Joseph NG Kee-yin presented the views as detailed in the submission of the Institution of Electrical and Electronics Engineers, Hong Kong Section (Computer Chapter).

Meeting with representatives of the Hong Kong Computer Society  
(LC Paper No. CB(2) 811/00-01(02))

4. Dr Louis MA presented the views as detailed in the submission of the Hong Kong Computer Society.

5. Mr Bill FOK informed Members that the word "escorted" as referred to in the third paragraph of the second page of the submission should read

"escrowed".

Meeting with representative of International Federation of the Phonographic Industry (Hong Kong Group)

(LC Paper No. CB(2) 811/00-01(03))

6. Mr Ricky FUNG Tim-chee presented the views as detailed in the submission of International Federation of the Phonographic Industry (Hong Kong Group) (IFPI).

Meeting with representative of the Hong Kong Information Technology Federation

(LC Paper No. CB(2) 832/00-01(01))

7. Mr LEE Kheng-joo presented the views as detailed in the submission of the Hong Kong Information Technology Federation (HKITF).

Meeting with representatives of the Hong Kong Society of Accountants and the Hong Kong Information Systems Audit and Control Association (Hong Kong Chapter)

(LC Paper No. CB(2) 828/00-01(02))

8. Mr Michael CHAN, Mr Peter TISMAN, Mr William GEE and Ms Susanna CHIU presented the views as detailed in the joint submission of the Hong Kong Society of Accountants and the Hong Kong Information Systems Audit and Control Association (Hong Kong Chapter).

Meeting with representatives of the Hong Kong Institution of Engineers (Information Technology Division)

(LC Paper No. CB(2) 828/00-01(03))

9. Ir Jolly WONG presented the views as detailed in the submission of the Information Technology Division of the Hong Kong Institution of Engineers.

Meeting with representatives of the Webmaster (Hong Kong) Association

(LC Paper No. CB(2) 811/00-01(04))

10. Mr Ringo LAM presented the views as detailed in the submission of the Webmaster (Hong Kong) Association.

Meeting with Mr Wanbil LEE

(LC Paper No. CB(2) 828/00-01(04))

11. Mr Wanbil LEE presented the views as detailed in his submission for the meeting.

Meeting with representative of the Information Security and Forensic Society  
(LC Paper No. CB(2) 841/00-01(01))

12. Mr Ricci IEONG presented the views as detailed in the submission of the Information Security and Forensic Society.

Issues raised by Members

13. Mr Howard YOUNG pointed out that HKITF suggested that the log records of accounts be kept by Internet service providers (ISPs) for less than three months, while the Webmaster (Hong Kong) Association considered that keeping the log records for a longer time would not result in a substantial increase in cost for ISPs. He asked about the rationale for keeping log records for a period of less than three months.

14. Mr LEE Kheng-joo responded that according to past experience and in consultation with HKISPA, HKITF considered that keeping a log record for three months was sufficient and feasible. Mr Howard YOUNG expressed concern that keeping the log records for three months or less might not be sufficient, as computer-related crime sometimes took a long time to detect.

15. Mr SIN Chung-kai said that computer-related crime might be difficult to define, as a person could use a local computer to activate a computer in overseas to hack a computer system in Hong Kong. He expressed concern that the Report had been compiled by the Inter-departmental Working Group on Computer Related Crime (the Working Group) without the assistance of the business sector and professional associations. He sought the attending deputation's views on whether the Administration should refer the issues raised in the Report to the Fight Crime Committee (FCC) for further examination. He added that while legislative amendments on computer-related crime might offer more protection, it might also hinder information technology (IT) development. Given that the subject of jurisdictional rules was still to be studied, he asked how computer related crime should be addressed and whether it was the appropriate time to introduce legislative amendments.

16. Deputy Secretary for Security (Special Duties) (DS for S(SD)) responded that the Administration would analyse the views received in the consultation exercise before determining the way forward. She said that even if the legislative amendments were to be introduced as proposed in the Report, it would be unlikely that a single piece of legislation would be introduced. While some legislative amendments could be introduced earlier, other legislative amendments such as those related to encryption might need more time to study. Bodies such as The Law Reform Commission would also take at least two to three years to study the jurisdictional rules.

17. Mr Chester SOONG considered that the issues raised in the Report

should be referred to FCC for further examination and consultation with the relevant parties should be conducted. This would assist the Government in better assessing the situation before the introduction of legislative amendments.

18. Mr Ricky FUNG Tim-chee said that besides the introduction of legislation on computer related crime, the Copyright Ordinance should also be amended.

19. Mr Ringo LAM commented that the Report had placed too much emphasis on legislative amendments. He considered that instead of forming different inter-departmental working groups to address different subjects such as computer-related crime, Internet gambling and copyright on the Internet, a new institution should be established under the Information Technology and Broadcasting Bureau (ITBB) to coordinate all work and address issues related to computer related crime and the Internet, including copyright on the Internet. He informed Members that legislation on copyright in the United States had been found inadequate for addressing copyright problems on the Internet. Many pieces of legislation had thus been enacted in the area in recent years. Ms Elizabeth QUAT said that the establishment of such an institution under ITBB would be more effective than the current arrangement of addressing problems on a piece meal basis.

20. Mr Bill FOK considered that instead of placing too much emphasis on legislative amendments at this stage, public education on information security should be stepped up.

21. Mr LEE Kheng-joo said that existing legislation had already set out the foundations for addressing various crimes. Discussions on computer-related crime would be ongoing. It was thus not possible to have one piece of comprehensive legislation on computer-related crime.

22. Mr Michael CHAN supported the view that an institution should be established under ITBB. He said that such a suggestion had been made by the Hong Kong Society of Accountants in the past when ITBB was first established. He added that both short-term and long-term solutions were needed for addressing the problem of computer related crime.

23. Mr William GEE said that it was difficult for the enactment of legislation to catch up with the rapid development of technology. Besides the enactment of legislation, everyone had a responsibility to safeguard the security of his own computer system. Codes of practice on computer security should be drawn up by the relevant professional bodies and organisations. Public education on information security should also be strengthened.

24. Dr Joseph NG said that as the enactment of legislation would take time, public education should be stepped up. He added that actions should be taken

in respect of short-term solutions identified in the Report, while the more fundamental issues could be examined at the same time.

25. Ms Audrey EU sought the views of attending deputations on the problem of Internet gambling. She asked whether it was technically viable to address the problem.

26. Mr LEE Kheng-joo said that it would be very difficult to take actions against bookmakers located overseas. Dr Joseph NG said that although it was technically viable to block certain web sites, offenders could easily establish another site on the Internet. He considered that little could be done in respect of enforcement against Internet gambling. Public education might be a more effective means in addressing the gambling problem. Mr Ricci IEONG said that the blocking of a web site would need the collaborative effort of all local universities and ISPs. Mr William GEE said that although the blocking of a web site would need the collaborative effort of all parties concerned, the question of who should be responsible for coordinating the blocking of a web site would have to be considered. He added that even if access to an overseas web site was completely blocked, a user could still establish connection with an overseas web site by means of a long distance call. It was thus very difficult to prevent Internet gambling. He considered that it would be more effective to address the problem through other means.

27. DS for S(SD) said that the Working Group had focussed its work on the macro problems of computer-related crime, such as encryption, jurisdictional rules and the adequacy of resources of law enforcement agencies. With the very rapid development of computer technology, the examination of all crimes that might be committed via the computer or the Internet, such as Internet gambling and pornographic materials, would be an endless task. Thus, the Working Group did not seek to deal with all crimes that might be committed via the computer or the Internet. They would be dealt with under the relevant policy context by the respective policy beaux concerned. She added that the Working Group comprised representatives from various government bureaux and departments, including ITBB. As regards denial of service, she said that prosecution had been made in the past under the Crimes Ordinance. However, it might not be possible under existing legislation to prosecute overseas hackers because of the jurisdictional problem.

28. Mr Ringo LAM said that from the perspective of a general public, he was concerned that the meaning of national security was unclear. He added that one might unintentionally breach the laws of the Mainland, as most people had little knowledge about Mainland laws.

29. Miss Margaret NG said that in the promotion of IT, it was important to create a safe environment that facilitated the privacy and freedom from surveillance. She considered that the recommendation in the Report in respect

of decryption was unacceptable. There should be a balance between protection against crime and the maintenance of a safe environment. With the compulsory disclosure of decryption tools or decrypted text and the maintenance of log records by ISPs, a safe environment could not be achieved because all users would be exposed to total surveillance. She hoped that a code of practice would soon be developed to facilitate a safe environment that provided protection against both crime and surveillance. She expressed concern that computer-related crime was suggested to be so broadly defined that innocent persons might be wrongly criminalised. In her view, it was important to ensure that compliance was viable before an act was criminalized. Problems related to jurisdictional rules should be dealt with speedily. As regards extraterritorial gambling, she said that the issue was being studied by the Bills Committee on Gambling (Amendment) Bill 2000. She invited the views of deputations on the drawing up of a code of practice to build up a safe environment.

30. Mr Bill FOK said that codes of practice were practical solutions to problems especially given that the enactment of legislation would take some time. In fact, there were already well established codes of practice and guidelines that complied with international standards in Hong Kong, although the majority of people in Hong Kong had not paid much attention to such codes.

31. Ms Susanna CHIU said that the removal of an offending web site should be carried out by the Commercial Crime Bureau of the Police rather than ISPs. She added that the commercial sector and the public seldom paid attention to codes of practice. Many small or medium sized companies lacked resources to introduce information security measures. Legislation were thus needed for a deterrent effect.

32. Mr William GEE said that as the environment of Internet was an insecure one, encryption and surveillance were needed for ensuring safety. He said that although closed circuit television systems could be found in many companies, they were intended for creating a deterrent effect rather than genuine surveillance. He added that codes of practice would facilitate building up a safe environment. He said that many codes of practice, best practices and guidelines were already in place in Hong Kong. Many international standards, such as ISO 17799, were under development. However, it was not possible to apply one single code of practice across different industries. The code of practice that should be adopted might be different from one industry to another. He added that besides putting in place codes of practice, a third party was also needed for monitoring compliance with the codes.

33. Mr Ricci IEONG said that the keeping of log records by ISPs was necessary because one could not know the identity of the person to whom communication was made. He informed Members that a hacker was found to have used the IP address of his former colleague to hack a certain important infrastructure. Without the log, it would have been very difficult to identify

who had performed the hacking. As regards denial of service, he said that existing legislation might not be adequate for dealing with situations where a hacker merely brought a system to a halt.

34. Mr Ricky FUNG Tim-chee said that although codes of practice were useful, IFPI hoped that legislation on "take down" procedures would be enacted.

35. Mr LEE Kheng-joo said that there was a lot of exchange between local and overseas ISPs on codes of practice. There was also peer group pressure for compliance with the codes of practice.

36. Mr Wanbil LEE said that the computer was a good tool in that it could extend one's intellectual power, although whether it would benefit or cause harm to the community would depend on how it was used. As regards blockage of web sites, it would be necessary to examine the information in the web site before a decision was made on whether blockage should be carried out. He said that the enactment of laws was always lagging behind events. While the discussions at the meeting had focussed on solutions and implementation aspects, he considered that the problem should be more clearly defined. As the process would be a lengthy one, short-term solutions should be introduced for the time being in parallel with the examination of the problem in a systematic way.

37. Mr James TO expressed concern that section 33 of the Telecommunications Ordinance had not been implemented after its enactment in 1997. He sought the views of deputations on whether there were legislative measures that should be introduced within a year's time. The Chairman said that the attending deputations could provide a written response after the meeting.

38. DS for S (SD) said that she believed that both the Administration and attending deputations shared the view that a good environment conducive to the legitimate use of the computer and the Internet should be provided. She pointed out that although the first few chapters of the Report focussed on legislative measures, the recommendations of the Working Group were not confined to such measures. The Working Group had in fact pointed out that administrative measures, which would require more sustained effort to implement, might be more effective in addressing the problem. Nevertheless, legislative measures would serve as a safety net.

39. The Chairman thanked the deputations for attending the meeting. He welcomed the deputations to provide further views, if any, to the Panel in writing.

40. The meeting ended at 12:05 pm.

Legislative Council Secretariat  
17 July 2001