立法會
Legislative Council

LC Paper No. CB(1)1382/05-06
(These minutes have been seen by the Administration)

Ref : CB1/PL/ITB/1

Panel on Information Technology and Broadcasting

Minutes of meeting
held on Friday, 17 March 2006, at 9:00 am
in Conference Room A of the Legislative Council Building

Members present	**:**	Hon SIN Chung-kai, JP (Chairman) Hon Albert Jinghan CHENG (Deputy Chairman) Hon Fred LI Wah-ming, JP Dr Hon LUI Ming-wah, SBS, JP Hon Jasper TSANG Yok-sing, GBS, JP Hon Howard YOUNG, SBS, JP Hon Emily LAU Wai-hing, JP Hon Timothy FOK Tsun-ting, GBS, JP Hon Ronny TONG Ka-wah, SC
Member attending	**:**	Hon James TO Kun-sun
Public officers attending	**:**	Agenda Item IV Mr Howard C DICKSON Government Chief Information Officer Mr Stephen MAK, JP Deputy Government Chief Information Officer (Operations) Ms Apollonia LIU Principal Assistant Secretary for Security E Miss Joanna CHOI Principal Assistant Secretary for Home Affairs 2

Agenda Item V

Mrs Marion LAI, JP
Deputy Secretary for Commerce, Industry and Technology (Communications and Technology)

Mr Tony LI
Principal Assistant Secretary for Commerce, Industry and Technology (Communications and Technology)B

Mr SO Tat-foon
Assistant Director of Telecommunications (Support)

Agenda Item VI

Mr Francis HO, JP
Permanent Secretary for Commerce, Industry and Technology (Communications and Technology)

Mrs Marion LAI, JP
Deputy Secretary for Commerce, Industry and Technology (Communications and Technology)

Agenda Item VII

Mr Howard C DICKSON
Government Chief Information Officer

Mrs Betty FUNG, JP
Deputy Government Chief Information Officer (Planning and Strategy)

Mr Stephen MAK, JP
Deputy Government Chief Information Officer (Operation)

Mr Victor LAM
Assistant Government Chief Information Officer (Digital 21 Policy and Strategy)

Attendance by Invitation : Agenda Item IV

Independent Police Complaints Council

Mr Ronny WONG Fook-hum, SC, JP
Chairman

Hon LEONG Kah-kit, SC
Vice – chairman

Mrs Brenda FUNG
Secretary

Office of the Privacy Commissioner for Personal Data, Hong Kong

Mr Roderick B WOO, JP
Privacy Commissioner for Personal Data

Ms Brenda KWOK
Chief Legal Counsel

Mr K T CHAN
Chief Personal Data Officer

Hong Kong Computer Emergency Response Team Coordination Centre

Mr Roy KO
Manager

Agenda Item V

Hong Kong Computer Society

Mr Allan DYER
Member, Information Security Division

Hong Kong Internet Service Providers Association

Mr Lento YIP
Vice Chairman

Ms Yvonne CHIA
Legal Adviser

Hong Kong and Mainland Software Industry Cooperation Association

Mr Joe LUO
President

Internet and Telecom Association of Hong Kong

Dr Yan XU
President, Regulation Issues Group

The British Computer Society (Hong Kong Section)

Dr P T HO
Honorary Consultant

The Institute of Electrical and Electronics Engineers Hong Kong (CAS/COM Joint Chapter)

Mr Y W LIU
Committee Member

Clerk in attendance : Miss Polly YEUNG
Chief Council Secretary (1)3

Staff in attendance : Ms Connie FUNG
Assistant Legal Adviser 3

Ms Debbie YAU
Senior Council Secretary (1)1

Ms Guy YIP
Council Secretary (1)1

Ms Sharon CHAN
Legislative Assistant (1)6

Action

I Confirmation of minutes and matters arising

(LC Paper No. CB(1)1004/05-06 -- Minutes of meeting held on 13 February 2006)

The minutes of the meeting held on 13 February 2006 were confirmed.

II Papers issued since last meeting

2. Members noted that no information paper had been issued since last meeting.

III Date and items for discussion for next meeting

(LC Paper No. CB(1)1071/05-06(01) -- List of outstanding items for discussion

LC Paper No. CB(1)1071/05-06(02) -- List of follow-up actions)

3. The Chairman explained that he would be out of town and would not be able to chair the next meeting on 10 April 2006. He suggested that the meeting should be held as originally scheduled and chaired by the Deputy Chairman; or be re-scheduled. Members agreed to consider the meeting arrangement under agenda item VIII : "Any other business".

IV Information Security

(LC Paper No. CB(1)1097/05-06(01) -- Information paper provided by Administration

LC Paper No. CB(1)1093/05-06(01) -- Newspaper cuttings on incidents involving leakage of personal data information on the Internet

LC Paper No. CB(1)1096/05-06(07) (*tabled and subsequently issued on 20 March 2006)* -- Questions from Hon SIN Chung-kai on "Information Security")

Introduction by the Administration

4. At the invitation of the Chairman, the Government Chief Information Officer (GCIO) informed members that the Office of the Government Chief Information Officer (OGCIO) took an active role in devising policies and providing support to bureaux/departments (B/Ds) as well as to the public on matters concerning the use of information and communication technologies. In doing so, OGCIO was mindful of the need to ensure that private and confidential data were protected. The Deputy Government Chief Information Officer (Operations) (DGCIO(O)) then took members through the measures facilitated by OGCIO on information security. He advised that under the Digital 21 Strategy for information and communications technology (ICT) development, establishing a secure environment was one of the key enablers in the promotion and development of ICT in Hong Kong. Hong Kong had put in place a comprehensive legal framework and an information security infrastructure to protect against and deal with computer-related crimes and misuse of personal information. Relevant initiatives included the scheme for certification authorities and the issuance of digital certificates under the Electronic Transactions Ordinance (Cap. 553), setting up of the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), the option of including a recognized digital certificate in the Multi-Application Smart ID Card and the two-factor authentication for high-risk

retail Internet banking transactions.

5. On the internal information security framework of the Government, DGCIO(O) said that the Government had developed a comprehensive set of information security policy and guidelines with reference to international best practice for use by B/Ds. At the departmental level, each department was required to appoint a senior officer to be in charge of the overall information security management and operation of the department. In addition, an Information Security Incident Response Team was set up in every department to deal with all matters on a day-to-day basis relating to security incident reporting and response.

6. On support to the industry and the public, DGCIO(O) advised that the setting up of the HKCERT in 2001 had enhanced Hong Kong's information security incident response capability. In 2002, the OGCIO set up a web site at www.infosec.gov.hk to provide a one-stop portal to facilitate public access to various information security related resources and updates. In 2005, the Internet Infrastructure Liaison Group was set up to facilitate local Internet stakeholders to share information and deal with incidents relating to the Internet in a coordinated way. He assured members that in 2006-2007, the OGCIO would continue its work to enhance the awareness and preparedness within the Government and in the wider community to deal with information security issues, including the updating of information security regulations, policies and guidelines and the promotion of and public education on the wider use of information technologies and information security.

Submission of views by related organizations

7. The Chairman welcomed the representatives of related organizations to the meeting. He noted that due to other commitment, Hon Ronny WONG, Chairman of the Independent Police Complaints Council (IPCC) and his colleagues might need to leave the meeting before 10 am. He also invited members to note that Hon Alan LEONG would attend this discussion session in the capacity of the Vice-Chairman of IPCC. The Chairman then invited the representatives to give views on issues related to information security and the incident concerning the leakage of personal data on the Internet.

Independent Police Complaints Council (IPCC)
(LC Paper No. CB(1)1096/05-06(05) -- Submission)
(*tabled and subsequently issued on 20 March 2006)*

8. Mr Ronny WONG, the Chairman of IPCC conveyed IPCC's sincere and unreserved apology to the public for the leakage of personal data of complaints against the Police. He explained that the cause of leakage hinged on the conversion of data furnished by the Complaints Against Police Office (CAPO) to IPCC. Since 2003, CAPO had provided case data to IPCC in the form of a CD-disc containing cumulative and updated information of complaints. However, the IPCC Secretariat had, on a number of occasions, experienced difficulties in

accessing the data stored in the CD-discs. The system maintenance contractor was called upon to render services of converting the data to enable the IPCC Secretariat to access the information. As revealed in the initial findings, the contractor had, for his own convenience, uploaded the data he obtained from IPCC onto a FTP server to facilitate his working at his office/home. The contractor however did not realize that no password was required to access or download the same. However, the information became accessible on the Internet. The Chairman of IPCC said that after the incident, IPCC had taken immediate remedial actions to rectify the situation and was also considering other remedial measures to step up its internal control of information security.

Office of the Privacy Commissioner for Personal Data, Hong Kong (PCO)
(LC Paper No. CB(1)1093/05-06(02) -- Submission)
(*tabled and subsequently issued on 20 March 2006)*

9. Mr Roderick WOO, Privacy Commissioner for Personal Data (the Privacy Commissioner) confirmed that PCO was in the course of following up with the cases concerning the leakage on the Internet of complainants' personal data held by IPCC and customers' personal data held by some other private organizations, including a telecommunications operator and an insurance company. Regarding the leakage of personal data held by IPCC, PCO had requested the relevant website operators including the newsgroup.com.hk, to take steps to remove such data from the Internet. He said that as investigation on the case was still in progress, it was not appropriate for him to disclose further details. However, upon completion of the investigation, a report would be published as soon as practicable.

10. Ms Brenda KWOK, Chief Legal Counsel of the Office of the Privacy Commissioner for Personal Data (CLC/PCO) then briefed members on the legal provisions concerning personal data security provided under the Personal Data (Privacy) Ordinance (Cap. 486) (PD(P)O). She advised that according to Data Protection Principle (DPP) 4 in Schedule 1 of PD(P)O, all reasonable practicable steps should be taken to ensure that personal data held by a data user were protected against unauthorized or accidental access, processing, erasure or other use. Regarding the leakage of personal data, she said that DPP1 stipulated that personal data should only be collected for a lawful purpose directly related to the data user's function or activity and the personal data collected should be necessary, adequate but not excessive. The means of collection should be lawful and fair in the circumstances of the case. Another principle, DPP3, provided that personal data should only be used for the purposes for which they were originally collected or for a directly related purpose unless the prescribed consent of the data subject was obtained. She pointed out that as the personal data contained in the IPCC database was for internal use only, any unlawful collection from the Internet or subsequent use of the data so obtained would be in breach of DPP1 and/or DPP3.

11. Regarding the penalty for contravention of DPPs, the Privacy Commissioner and CLC/PCO advised that the present scheme under PD(P)O was not to make it a direct offence for infringement of the DPPs. It was only upon the issuance of an

enforcement notice and the failure to comply with such a notice that an offence would be committed. Moreover, currently, the Privacy Commissioner was not conferred with criminal investigation and prosecution powers under PD(P)O. As the PD(P)O had been in force for nearly a decade, the Privacy Commissioner remarked that it was now time to review the PD(P)O.

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)

12. Mr Roy KO, Manager, HKCERT informed members that according to the International Organization for Standardization (ISO), a comprehensive set of controls comprising best practices in information security was provided in ISO17799. Under ISO17799, guidelines and procedures were laid down for many facets, such as those on data classification and control, system access control, security and risk management, and data transfer.

Discussion

Role of the Privacy Commissioner and review of PD(P)O

13. Mr Ronny TONG was concerned whether the parties concerned had breached provisions in PD(P)O under the circumstances below :

(a) Before passing the information to the contractor, IPCC had failed to ensure that the contractor would handle the personal data received from IPCC with due care.

(b) the contractor had uploaded the personal data received from IPCC to the FTP server, apparently without notifying or obtaining authorization from IPCC and without taking all practical steps to ensure that no information would be leaked.

(c) The server of Goggle, a major search engine, had been used as a tool in searching and disseminating personal data held by IPCC.

14. In response, the Privacy Commissioner and CLC/PCO highlighted PCO's stance that since investigation of the IPCC case was underway, they were not in a position to comment on whether the various parties had breached the PD(P)O or otherwise. CLC/PCO further advised that pursuant to Principle 4 in Schedule 1 to the PD(P)O concerning "security of personal data", a data user should take all reasonably practicable steps to ensure that the personal data held by it were protected against unauthorized access, such as by specifying the security requirements for handling personal data in the relevant contract with the contractor.

15. Mr Ronny TONG did not subscribe to the Privacy Commissioner's stance against providing comments on the IPCC case pending investigation. He referred to the role of PCO in promoting privacy protection and considered that it should take a proactive role in educating the public on observing the set of DPPs under PD(P)O. He noted that section 4 of PD(P)O provided, inter alia, that "a data user

shall not do an act, or engage in a practice, that contravenes a data protection principle"; while according to section 64(10), a data user who, without reasonable excuse, contravened any requirement under PD(P)O for which no other penalty was specified in section 64 committed an offence and was liable on conviction to a fine at level 3. Mr TONG was thus concerned whether the Privacy Commissioner had sought legal advice on whether contravention of a DPP would constitute a contravention of the requirement under section 4 of PD(P)O, and if so, whether such contravention would amount to an offence as provided under section 64(10); and whether the Privacy Commissioner could exercise his power to investigate and/or even prosecute those who had contravened a DPP.

16. In response, the Privacy Commissioner recapped that currently, he was not equipped with prosecution powers. CLC/PCO further clarified that failure to comply with a data access request under section 19 or non-erasure of personal data no longer required under section 26 would amount to an offence but infringement of DPPs *per se* did not give rise to an offence. It was only upon the issuance of an enforcement notice and subsequent failure to comply with the terms of the enforcement notice that an offence would be committed. In fact, section 64(10) of PD(P)O had expressly excluded contravention of DPPs from the scope of offence provided in the said section. The Privacy Commissioner considered that PD(P)O was very clear on the scope of the Commissioner's power and the offence provisions and as such, there was no proven need to seek an independent legal advice on these issues. He nevertheless took note of Mr Ronny TONG's view and would give consideration to the necessity of seeking independent legal advice should the Chairman of the Panel request him to do so.

17. The Privacy Commissioner explained that if a data user had failed to comply with the enforcement notice issued to him/her under section 50 of PD(P)O, the Privacy Commissioner would need to forward a detailed report to the Hong Kong Police for investigation. If the offence was substantiated, the Department of Justice would be asked to consider taking prosecution action under section 64(7) of the Ordinance. The Privacy Commissioner considered that under the present arrangement, there might be duplication of investigation effort resulting in unnecessary delay in the prosecution of substantiated cases. He remarked that since protection of privacy right was a new concept when introduced in the 1990s, it appeared that the legislative intent at that time was not to impose serious punishment. Now that the Ordinance had been in force for nearly a decade, it was time to review whether more serious punishment should be imposed on infringement of the Ordinance and whether the Privacy Commissioner should be conferred with criminal investigation and prosecution powers.

18. Ms Emily LAU supported a review of PD(P)O and urged the Home Affairs Bureau (HAB) to proceed with the review expeditiously. If PCO could demonstrate a need to strengthen its work, she said that HAB should consider allocating more resources to PCO, if necessary. Ms LAU shared Mr Ronny TONG's view that the Privacy Commissioner should, as far as possible, play a more proactive role in promoting privacy protection.

19. In view of the limitations under the existing legislation, Mr Fred LI also expressed support for a review of PD(P)O to provide the Privacy Commissioner with criminal investigation and prosecution powers. He pointed out that in the IPCC case, although the information had been pulled out of the websites concerned, it was still accessible and had been posted to newsgroups for downloading using the BT technology. Mr LI was worried that the leakage would continue and run out of control. Given that the advent in information and communications technology had posed new challenges to the scope, transmission, use and protection of personal data, Mr LI stressed that it was timely to review the Ordinance to assess its efficacy or otherwise in the face of technological advancement in the electronic age.

20. In this connection, the Principal Assistant Secretary for Home Affairs 2 confirmed that the Administration was looking into the suggestions raised by the Privacy Commissioner on criminal investigation and prosecution powers. Follow-up action would be taken upon receipt of recommendations from the Privacy Commissioner regarding the review of whether more serious punishment should be imposed on infringement of the PD(P)O. Ms Emily LAU suggested that the Panel on Home Affairs should be requested to follow up with the Administration and the Privacy Commissioner on the review of the Ordinance, preferably in two to three months' time. Members agreed.

(*post-meeting note:* The Clerk has relayed members' request to the Clerk to Panel on Home Affairs in writing on 20 March 2006.)

Information security protection measures adopted by IPCC

21. Mr Ronny TONG was concerned whether IPCC had included any provision in the agreements to require the contractor to handle the personal data received from IPCC in confidentiality and with due care.

22. In response, the Chairman of IPCC explained that in 1998, IPCC entered into an agreement with the EDPS Systems Limited (EDPS) to set up a stand-alone system containing information about complaints against the Police for statistical and research purposes. The agreement did not contain any express terms in relation to the protection of personal data and the secure transmission of the data. Subsequent system maintenance and enhancement contracts had been awarded to EDPS since 1999. However, EDPS had subcontracted the maintenance work to a former employee who had been involved in the design and development of the system. The Chairman of IPCC said that IPCC had not been informed of the subcontracting and he considered the arrangement inappropriate.

23. Mr Ronny TONG further enquired whether it was incumbent upon IPCC to make sure that its contractor would take all necessary precautionary measures to ensure the secure transmission of the personal data received from IPCC.

24. In response, the Chairman of IPCC stated his view in the affirmative. He referred to a circular issued by the IPCC Secretariat on 20 August 1998 advising all

IPCC Secretariat staff to take reasonable care to safeguard at all times the security of office property and documents in their care. The circular had also specified that the Senior Assistant Secretary in the office was designated as the Departmental Security Officer responsible for overseeing the security arrangement for the protection of documents and information, among other things. He considered it very unfortunate that one of the Secretariat staff members had failed to observe the guidelines.

25. In response to Mr Ronny TONG's further query on the parties that should be held responsible for approving the contract with EDPS without including any security requirement on the handling of confidential personal data, the Chairman of IPCC said that IPCC had the overall responsibility. However, he pointed out that before approving the agreement with the contractor in question in 1998, the IPCC Secretariat had sought the advice of the former Information Technology Services Department (ITSD). ITSD had given general comments on the proposed tender and the contract terms relating to the technical aspects of the information system. However, it had not raised any express comments relating to the protection of personal data.

26. On the parties who had signed the agreements on behalf of IPCC, Mrs Brenda FUNG, Secretary of IPCC recalled that the first contract on the development of the stand-alone system in 1998 might have been signed by the then Secretary of IPCC whereas other staff in the Secretariat might have signed subsequent agreements on system enhancement or maintenance. In this connection, DGCIO(O) said that while the former ITSD had provided technical advice to user departments or related organizations on the development of information systems, it had also formulated comprehensive information technology (IT) security policies, procedures and relevant guidelines to enable B/Ds as well as related organizations to build up their own information security systems and practices. They were also required to comply with the Government's Security Regulations (SR). There was a dedicated section in the SR covering information systems and related topics on storage, processing and transmission of information, including classified information, cryptographic key management, physical security, and proper destruction of classified information. DGCIO(O) said that the ITSD might not have been given the full contract to comment on in the first place. He understood that ITSD had also provided advice to the IPCC Secretariat when it applied for funding to replace its computer in 2001. In this connection, the Chairman was gravely concerned that IPCC might have failed to comply with the Government's SR and follow the established procedures and guidelines in developing and maintaining their information systems.

27. Mr Howard YOUNG considered that the incident had damaged the credibility of IPCC. Noting that the contractor had converted the personal data provided by the IPCC Secretariat at his office/home by uploading onto an FTP server for his own convenience, Mr YOUNG was concerned whether such a way of handling personal data had violated the international best practices of handling sensitive data and whether the contractor, in so doing, had breached the contract terms. He also enquired about the extent of information that had been leaked.

28. The Chairman of IPCC highlighted that while there was no express provision in the contract about secure transmission of personal data provided by IPCC, the contractor was fully aware of the nature of IPCC's work. The Chairman of IPCC said that the subcontractor had admitted fault for the leakage and apologized to IPCC. On the extent of information leaked, the Chairman of IPCC reported that the information known todate involved the personal data, including their names and Hong Kong identity card (HKID) numbers, of about 20 000 people who had filed complaints against the Police, together with the coding of allegations and classifications of the complaint cases. He pointed out that most of the leaked data were past data, with seven on-going cases which were subject to review. The Chairman of IPCC called on the public to re-focus attention on IPCC's work to monitor the handling of complaints against the Police and not to lose confidence in IPCC because of a single incident.

29. The Deputy Chairman considered that the contractor in question had committed a serious mistake in violation of information security principles. He said that IPCC should consider terminating its agreement with the contractor. The Deputy Chairman was also very concerned as to why staff of the IPCC Secretariat had not noticed the leakage. Ms Emily LAU raised grave concern that according to some media reports, the leaked information had been circulated on the Internet for some three years.

30. In response, the Chairman of IPCC recapped that in 2003-04, the person who had been subcontracting the conversion work had uploaded the personal data provided by IPCC to an FTP server without the consent or knowledge of the IPCC Secretariat staff. They did not know about the matter until the incident was reported in the press on 10 March 2006. According to IPCC's investigation, 1 218 files containing the personal data of about 20 000 complainants and eight sub-folders of text files were involved in the leakage. The Chairman of IPCC further said that in view of the seriousness of the leakage in question, IPCC was actively considering terminating the contractor's service.

Independent investigation and detailed report

31. Ms Emily LAU recalled that at the special Finance Committee meeting to examine the 2006-2007 Estimates, the Secretary of IPCC had responded to members that the IPCC Secretariat's staff had overlooked the absence of any provision on the security requirements in the agreements signed with the contractor. In Ms LAU's view, investigation by IPCC alone into its own affairs was not enough. Instead, she urged for an independent investigation into the incident, which would be more credible and objective. It could also help identify the parties to be held responsible for the leakage, the loopholes, if any, in the security procedures and come up with useful recommendations on how to safeguard the security of personal data held by IPCC.

32. While acknowledging the seriousness of the incident and IPCC's responsibility, the Chairman of IPCC informed members that IPCC had in fact set

up a four-member Task Force to investigate into the leakage, consider the remedies and take immediate action to prevent recurrence. The work of the Task Force was progressing well.

33. Ms Emily LAU was disappointed that IPCC did not support her suggestion for an independent committee to investigate into the incident but she still requested the Administration to consider her suggestion. Ms LAU further remarked that IPCC had not provided sufficient information in its paper to enable Panel members and the general public to fully understand the leakage incident. Ms LAU considered that IPCC should have provided a more detailed report, outlining, inter alia, the chronology of events leading to the incident, the seriousness of the problem and remedial actions.

34. In reply, the Chairman of IPCC advised that the paper aimed to provide a concise account of the incident for members' information. He would have no objection to providing a more detailed report. The Chairman of IPCC understood that the Privacy Commissioner would initiate an investigation into the matter. He and staff of the Secretariat had already met the Privacy Commissioner and would fully co-operate in the investigation. He added that Panel members might consider the need or otherwise for an independent investigation after the Privacy Commissioner had published his report.

35. Ms Emily LAU welcomed the investigation to be conducted by the Privacy Commissioner and urged him to carry out the investigation in a rigorous manner and to conduct hearings as and when necessary. She also requested the Privacy Commissioner to provide a copy of his investigation report to the Panel, with recommendations on his findings and further actions, such as whether any staff of the IPCC should be penalized.

36. In response, the Privacy Commissioner confirmed that PCO had taken the initiative to approach the IPCC and made enquiries on the circumstances leading to the incident. He had led officers of PCO to meet with the Chairman, Vice-chairman and the IPCC Secretariat. On when the report would be ready, the Privacy Commissioner advised that this would depend on the progress of investigation and in particular the extent of co-operation rendered by the relevant parties. Nevertheless, he assured members that his office would handle the matter with top priority.

37. Dr LUI Ming-wah declared that he was a Vice-Chairman of IPCC. He considered that it was important to probe into the matter thoroughly with a view to preventing similar recurrence in Government and other organizations. However, as the matter did not involve commercial or individual interests, he considered that the investigations by IPCC and PCO would suffice. Dr LUI urged members to be forward-looking and considered it not very meaningful to track down the staff who should be held responsible for the incident.

38. The Chairman of IPCC shared Dr LUI's view that it was more important for IPCC to focus on lessons to be learnt from the incident. He noted that the officer

of the IPCC Secretariat who had failed to prevent unauthorized access to the personal data held by IPCC was currently seeking legal advice and would provide an explanation to IPCC in due course.

Independence of IPCC

39. The Chairman of IPCC referred to the good reputation of IPCC built up by the two former chairmen, Mr Robert TANG and Mr Denis CHANG over the years. He was disappointed to note that the credibility of the well-established mechanism in handling complaints against the Police had been undermined as a result of the present incident. The Chairman of IPCC nevertheless considered that from a longer-term perspective, the accountability and transparency of IPCC should be achieved by establishing a fully independent IPCC. Ms Emily LAU supported a truly independent IPCC and recalled that the United Nations Human Rights Committee had long been calling on the Government to set up a truly independent body to investigate into complaints against the Police. As such, she urged the Security Bureau (SB) to follow up the matter and expedite the preparation of the necessary legislative proposals.

40. In response, the Principal Assistant Secretary for Security E confirmed that to further improve the mechanism for reviewing the handling by the Police of complaints by the public, SB was in the process of discussing the details of a proposed bill with IPCC. In line with the established practice, SB would consult the Panel on Security before introducing the bill into the Council.

Remedial action for affected complainants.

41. Notwithstanding that the IPCC had offered a sincere and unreserved public apology, Mr James TO urged the IPCC to notify the 20 000 complainants whose personal data had been leaked directly through appropriate means such as personal letters to alert them of the possible misuse of their particulars by other people. In response, the Chairman of IPCC confirmed that the IPCC had considered this option at a meeting held earlier. Subject to the availability of manpower support provided by SB, the Chairman of IPCC said that it was very likely that IPCC would pursue this course of action.

42. The Deputy Chairman did not see the need for further consideration and took the view that the 20 000 complainants should be notified without delay as not all of them could be expected to be aware of the leakage of their personal data. The Chairman of IPCC, in response, further highlighted the difficulty in sending apology letters to complainants because serving police officers were also involved. IPCC was considering whether it might be more appropriate to make a direct apology to the Commissioner of Police instead. The Deputy Chairman suggested that IPCC should separate the complainants concerned into two groups and send personal letters to the general citizens.

43. Mr James TO was gravely concerned that the personal safety of an individual complainant might be jeopardized if his/her identity was exposed, in

particular if the complaint he/she had lodged was a serious one. As the number of such complainants would likely be very small, Mr TO urged the Administration to consider taking special action, such as changing the HKID card numbers of these complainants. While noting Mr TO's suggestion, the Chairman of IPCC confirmed that the complaint cases had been classified according to their sensitivity and would be dealt with in the most prudent manner.

Remedial action to deal with remaining traces of the leaked data on the Internet

44. Members noted that the IPCC had sought the GCIO's urgent advice on steps which could be taken to continuously track and delete the remaining traces of the data on the Internet, and to prevent further spreading of the data and ways to mitigate the damage. Mr James TO referred to the recent civil and criminal actions taken against unauthorized downloading of copyright works from the Internet by the music industry and the Administration respectively and enquired about the actions that would be taken by OGCIO to stop further spreading and downloading of the data from the Internet using applications such as BT software.

45. On ways to track and delete the remaining traces of data on the Internet, DGCIO(O) advised that the OGCIO had discussed with the Police, HKCERT, Internet service suppliers and expert groups on information security and concluded that while IPCC could analyze the traffic log to trace those Internet users who might have obtained the data, there was practical difficulty in removing the remaining traces of data entirely, especially when copies of the data might have been downloaded and kept. Separately, DGCIO(O) advised that certain services available overseas could enable an Internet search for targeted data in a most rigorous manner. However, as this type of service had its risks and might bring about unintended adverse results, OGCIO had not recommended its use to IPCC. In response to Mr James TO's urge for greater technical assistance to IPCC, DGCIO(O) confirmed that OGCIO would provide assistance to IPCC where necessary.

46. Noting members' concerns, GCIO highlighted that while resources could be used to track and delete remaining traces of the data, it was more important to ensure the adoption of the correct management practice in information security protection by the Government and non-government organizations which handled personal data.

47. Noting that IPCC had obtained cooperation from most of the search engine companies and Internet service providers in erasing the cache with the information in question, Mr Jasper TSANG was concerned whether this meant that a small number of companies had refused to erase the information. Mr TSANG also enquired whether IPCC had followed up the urgent advice provided by OGCIO and if yes, the progress achieved so far.

48. In response, the Secretary of IPCC elaborated that IPCC had contacted Google and other search engine companies and Internet service providers to appeal for their assistance in erasing the cache with the information. The cooperation

from most of them had been obtained. Although some of them had not provided a positive response to IPCC, recent search by IPCC showed that the information was no longer accessible from the cache. IPCC had followed the technical advice provided by OGCIO in tracking and causing deletion of the remaining traces of the data on the Internet. However, more recently, it was found that the information was still accessible and had been posted to newsgroups for downloading using the BT technology. She pointed out that apart from manpower constraint, IPCC also needed further technical support and advice. As such, IPCC had sought OGCIO's overall advice on the actions that could be taken to stop further circulation of the leaked information on the Internet.

49. DGCIO(O) confirmed that OGCIO had received IPCC Secretariat's request for advice on further action two days ago. Certain actions that could be taken had already been outlined earlier in the meeting. He pointed out that as the leaked information could still be accessed by way of different technologies, it was necessary to devise special measures to tackle illegal or unauthorized transmission, collection or use of the information via the Internet.

Remedial action to prevent recurrence

50. Referring to other remedial actions proposed by IPCC in paragraph 16 of its paper (CB(1)1096/05-06(05), Mr Jasper TSANG was concerned whether IPCC had sought the views of the Privacy Commissioner to see if they were adequate to prevent recurrence. Referring to the public education and publicity on the fight against corruption launched by the Independent Commission Against Corruption, Mr TSANG enquired whether the PCO also carried out similar public education programmes to disseminate information on the protection of privacy.

51. In response, the Secretary of IPCC pointed out that other remedial actions listed in paragraph 16 were proposed measures which would be forwarded to the Privacy Commissioner as part of IPCC's response to his investigation. The IPCC would comply with the Privacy Commissioner's recommendations given in due course.

52. On public education, the Privacy Commissioner highlighted that one of the PCO's tasks was to guide data users in handling personal data. The PCO had published information booklets, such as "A Guide for Data Users" "E-Privacy: A Policy Approach to Building Trust and Confidence in E-Business", "Personal Data Privacy and the Internet – A Guide for Data Users", which were available on PCO's website. In addition, the PCO also organized workshops and seminars from time to time to introduce provisions of PD(P)O and the compliance requirements. The Privacy Commissioner further advised that about three weeks' ago, he had called on Government departments, especially those which managed a large database of personal data, to fill out a questionnaire on privacy impact assessment. The Privacy Commissioner added that he also planned to implement by the end of the year a data-user registration scheme under which all data users would be required to register with PCO the prescribed particulars about the personal data collected, held, processed or used by them.

Summing up

53. The Chairman highlighted that as revealed by the incident, despite the availability of a comprehensive set of information security policies and guidelines modeled on best international practices for use by B/Ds and related organizations, it was vital for OGCIO to ensure that these parties and their contractors would duly follow the established policies and guidelines. Moreover, OGCIO should also ensure that regulatory bodies, such as the Office of Telecommunications Authority and Office of Commissioner of Insurance, would see to it that the industry players under their respective purviews would comply with information security practices and requirements.

54. Sharing the Chairman's view, GCIO agreed that the recent incidents of leakage on the Internet of personal data held by IPCC, a telecommunications operator and an insurance company were indeed primarily a question of information management. OGCIO would strive to enhance public awareness in managing personal information among data users within and outside the Government.

55. To facilitate members' consideration of how to follow up the leakage incident, members in general agreed that IPCC should be requested to provide a more detailed report to include the following:

(a) a chronology of events since 1998 leading to the incident;

(b) the details, such as the dates and parties involved in the agreements signed with the contractor(s) in question and consultation with the former ITSD (now OGCIO);

(c) guidelines issued to IPCC Secretariat staff on ways to ensure information security, such as the circular issued by IPCC Secretariat on 20 August 1998; and

(d) remedial actions that had been and would be taken.

56. The Chairman thanked representatives of the various organizations, in particular Mr Ronny WONG, Chairman of IPCC, for attending the meeting. He suggested that upon receipt of the said report from IPCC, he would discuss with Mr James TO, Chairman of the Panel on Security, on how the matter should be followed up. Members agreed.

(*post-meeting note* : The "Report on leakage of personal data" prepared by IPCC has been issued to all Members on 8 April 2006. The Chairman has advised that the Panel on Security has been invited to consider how the report should be followed up. It has also been requested that members of this Panel be invited to take part in the meeting of the Panel on Security, if held, to discuss the subject. Members have been duly informed of the

above on 10 April 2006 vide LC Paper No. CB(1)1278/05-06.)

V Public consultation on the legislative proposals to contain the problem of unsolicited electronic messages

LC Paper No. CB(1)1071/05-06(03)	-- Consultation paper on legislative proposals to contain the problem of unsolicited electronic messages
LC Paper No. CB(1)772/05-06(02)	-- Press release on 20 January 2006 on proposed anti-spam legislation
LC Paper No. CB(1)1072/05-06	-- Background brief on proposals to contains the problem of unsolicited electronic messages

Presentation by the Administration

57. With the aid of power-point presentation, the Principal Assistant Secretary for Commerce, Industry and Technology (Communications and Technology)B (PASCIT (CT)B) briefed members on detailed proposals of the Unsolicited Electronic Messages Bill (UEM Bill). He highlighted the following:

(a) The UEM Bill was drawn up having regard to six guiding principles aimed at striking a balance among the interests of different stakeholders. In gist, while the freedom of speech and expression and room for the development of e-marketing should not be stifled, the proposed Bill also sought to protect the right of an individual to decide whether to receive or refuse commercial UEMs.

(b) In view of the rapid development of information and communications technology, all forms of commercial UEMs, unless specifically excluded, would be regulated under the proposed Bill so as to cater for future development in technologies and services. In addition, due to the distinct cross-boundary nature of some of the UEMs, the Bill provided that even if the spamming act might occur outside Hong Kong, as long as the commercial UEM had a "Hong Kong link", then any related contraventions of the Bill should fall within the jurisdiction of Hong Kong.

(c) Senders of commercial UEMs would be required to provide a functional unsubscribe facility (i.e. the opt-out regime) to enable registered users of electronic addresses to notify the sender that he did not wish to receive further commercial electronic messages from that sender. Furthermore, "do-not-call registers" of appropriate types of electronic addresses would be maintained by the Telecommunications Authority (TA) to supplement the opt-out regime.

(d) Employers and principals would be held liable for the acts done or practices engaged by their employees and agents, unless they could prove that they had taken all practicable steps to prevent such acts or practices.

(e) For offences of a less serious nature, such as the sending of commercial UEMs to electronic addresses obtained by automated means, the penalty would be a fine up to $1,000,000 and imprisonment up to five years. For offences related to fraud, such as hacking and spamming through zombie computers, the offender would be liable on conviction to a fine of an amount as determined by the Court and to imprisonment up to 10 years. A person who contravened any provisions in the UEM Bill would also be liable to pay compensation to the victim for the pecuniary loss sustained as a result of the contravention.

(f) Different parts of the UEM Bill might commence on different dates to provide flexibility for e-marketers to gear up their equipment as well as to enable the Government to undertake public education activities.

Submission of views by deputations

58. Members noted that Mr LAU Hing-kee, a member of the Sai Kung District Council who did not attend the meeting, had provided a submission (LC Paper No. CB(1)1071/05-06(05) in response to the Administration's legislative proposal to contain the problem of UEMs.

Hong Kong Computer Society (HKCS)
(LC Paper No. CB(1)1093/05-06(03) -- Submission)

59. Mr Allan DYER, member of the Information Security Division of HKCS said that HKCS strongly supported the introduction of legislation in Hong Kong to control UEMs. For enforcement purpose, HKCS proposed to define a "registered user" as the person who paid for the email address. He then pointed out that it would not be justifiable to make the recipients responsible for verifying whether or not an unsolicited message was a commercial UEM before reporting it. On the opt-out regime, he said that some administrators would block messages from large blocks of addresses, such as the whole Internet Service Providers (ISPs). To provide room for the development of e-marketing, he considered that the Administration should try to prevent Hong Kong from being blocked by all overseas ISPs. Noting that the Administration had proposed to set up "do-not-call registers" in respect of telephone numbers only but not for emails where the problem was also very serious, he remarked that if the "do-not-email registers" simply listed the addresses, it was true that spammers could make use of the enormous list of valid email addresses contained in the registers to send messages by evading legal liability as long as they could make their messages untraceable. However, Mr DYER said that there was a technical solution to resolve the potential

problem by using the cryptographic technology to protect the registered content of a "do-not-email register" and the other types of "do-not-call registers".

Hong Kong Internet Service Providers Association (HKISPA)
(LC Paper No. CB(1)1071/05-06(04) -- Submission)

60. Ms Yvonne CHIA, Legal Advisor of HKISPA said that HKISPA appreciated the Administration's effort in taking forward feedbacks collected from previous consultations on containing the problem of UEMs. HKISPA, however, doubted whether spamming could be effectively curbed by merely regulating commercial UEMs. HKISPA also proposed to provide in the UEM Bill that ISPs could reject the transmission of UEMs on grounds that the normal network/facility operation would be impeded and to confer rights which were comparable to those under the CAN-SPAM Act of the United States (US) on local ISPs to commence civil actions. She further opined that the general prohibition in the UEM Bill against misleading subject headings was not enough and proposed that the labeling of "ADV" be made mandatory for commercial unsolicited email messages.

Hong Kong and Mainland Software Industry Cooperation Association (HMSICA)
(LC Paper No CB(1)1096/05-06(06) -- Submission)
(*tabled and subsequently issued to members on 20 March 2006)*

61. On behalf of HMSICA, Mr Joe LUO, President of HMSICA expressed support for the proposed UEM Bill. Apart from the comments highlighted in HMSICA's submission, he also expressed concern on the Administration's proposal that it was an offence to send multiple commercial UEMs through 'five or more electronic addresses by falsified identity of the actual registrant', the definition of which should be made clear in the proposed Bill so as to allow room for e-marketing development. He also urged the Administration to partner with the software industry to facilitate the development of software programmes to facilitate compliance with the UEM Bill by the commercial sector in a more automated manner.

Internet and Telecom Association of Hong Kong (ITAHK)
(LC Paper No. CB(1)1081/05-06(01) -- Submission)

62. Dr Yan XU, President of Regulation Issues Group of ITAHK said that ITAHK welcomed the Administration's consultation on legislative proposals to contain the problem of UEMs without impairing the freedom of speech and expression. Nonetheless, ITAHK urged the Administration to make a cautious balance between protecting the public from illicit spamming activities on the one hand and facilitating innovative applications of the Internet and other telecommunications system and technologies on the other hand. ITAHK considered it important to define UEMs, otherwise, the enactment of the Bill might generate unexpected controversies. In addition, Dr XU remarked that in view of the possible merging of the TA and the Broadcasting Authority and the integration of the Telecommunications Ordinance and Broadcasting Ordinance, the UEM Bill

should be drafted within this context with a view to fitting seamlessly with the future Communications Ordinance.

The British Computer Society (Hong Kong Section) (BCS(HK))
(LC Paper No. CB(1)1081/05-06(02) -- Submission)

63. Dr P T HO, Honorary Consultant of BCS(HK) said that given the widespread concerns of the general public about the nuisance caused by UEMs, BCS(HK) supported in principle the enactment of the UEM Bill. However, it was equally important that the development of Information and Communications Technology for commercial marketing purposes. To forbid commercial organizations from going beyond the legislative framework, he said that it was necessary to clarify in the proposed Bill the principle of freedom of speech and expression. BCS(HK) also considered that commercial organizations should be prohibited from releasing their customers' contact data to any third party without the consent of the data subjects. Furthermore, there should be some guidance/requirements for the commercial organizations to respond to the UEM recipients' complaints or opt-out requests. Dr HO further said that to facilitate enforcement, issues concerning the definition of commercial UEMs and how best the Bill would guard against UEMs from overseas entities should also be properly addressed.

The Institute of Electrical and Electronics Engineers Hong Kong (CAS/COM Joint Chapter) (IEEEHK)
(LC Paper No. CB(1)1096/05-06(04) -- Submission)
(*tabled and subsequently issued to members on 20 March 2006)*

64. Mr Y W LIU, Committee Member of IEEEHK said that IEEEHK generally supported the proposed Bill. He pointed out that the real commercial UEMs were not the major source of nuisance to UEM recipients because commercial organizations would not destroy their credibility by spamming their potential customers. In IEEEHK's opinion, the scope of the proposed legislation should also include individual illicit UEMs as they caused much nuisance to recipients. However, IEEEHK considered the "opt-in" and "opt-out" functions complicated, not effective and would only add to the burden of small companies. As such, IEEEHK would not support the Administration's proposal to mandate an "opt-out" mechanism on senders of commercial electronic messages.

Discussion

Safeguarding freedom of speech and expression

65. Ms Emily LAU was pleased to note that deputations were in support of one of the guiding principles underlying the proposed legislation that freedom of speech and expression must not be impaired. She sought explanation from the Administration as to how it could uphold freedom of speech and expression while regulating the transmission of commercial UEMs. Ms LAU also asked whether

the query would arise as to why senders of commercial electronic messages could not enjoy the same extent of freedom of speech and expression as senders of non-commercial electronic messages.

66. In response, DSCIT(CT) explained that in line with the Government's light-handed regulatory approach and with reference to overseas practices, the Administration aimed to target the proposed legislation at UEMs of a commercial nature only because they caused the most problems. She recapped that any electronic message which purported to offer, advertise, promote, or sponsor the provision of goods, facilities, services, land or a business or investment opportunity etc. would be defined as commercial electronic messages. On the guiding principle in relation to freedom of speech and expression, DSCIT(CT) acknowledged the rights of the sender to disseminate information on its products and services, but such rights should be subject to reasonable limits. The proposed opt-out regime was an arrangement which would not prohibit the transmission of commercial electronic massages altogether, and at the same time safeguard the recipients' freedom in deciding whether to receive or refuse such commercial information.

67. Mr Jasper TSANG expressed support for the proposed opt-out regime which in his opinion had struck a balance between freedom of expression and the recipients' choice.

"Do-not-call registers"

68. Given that the recipient of an UEM sent via interactive voice response system (IVRS) technology might have to pay hefty roaming charges if he was outside Hong Kong when answering the call, Mr Jasper TSANG enquired whether it was technically feasible for the caller to ascertain from the signals of the recipient's mobile phones whether the recipient was in Hong Kong or overseas; and to stop the call if the recipient was outside Hong Kong.

69. In response, AD/Tel(S) advised that while the telecommunications operators might be able to track the location of their mobile phone service users, they could not ascertain whether the calls in question were UEMs. AD/Tel(S) further said that although senders of commercial UEMs using IVRS could partner with telecommunications operators to enable the latter to differentiate the calls, such service was not available in the market at present. AD/Tel(S) further advised that the purpose of setting up the "do-not-call registers" for the appropriate types of electronic addresses was to supplement the functional unsubscribe facility requirement for the opt-out regime. E-marketers should avoid sending commercial electronic messages to persons whose telephone numbers had been placed in such "do-not-call registers" irrespective of whether they were within or outside Hong Kong.

70. Considering that most mobile phone recipients of commercial UEMs were concerned about the unfairness of charges being incurred on them as a result of answering the calls, Mr Howard YOUNG reiterated his suggestion of a "calling

party pays" option under which senders of commercial UEMs, instead of the recipients, would pay the airtime/roaming charges thus incurred. In response, AD/Tel(S) recapped the technical problem that telecommunications operators could not ascertain the nature of the calls and re-direct the charges to the caller as proposed by Mr YOUNG. While the recipients might choose to disable the roaming function on their mobile phones but it also meant that other legitimate calls would also be blocked.

Admin

71. While agreeing that the "do-not-call registers" of telephone numbers would be helpful in curbing UEMs sent via IVRS technology, the Chairman was worried that with the increasing take-up of IP telephony by the public, the registers, which were databases of valid telephone numbers, would be abused by overseas spammers who would make unsolicited calls to Hong Kong through IP telephony to those registered numbers. Notwithstanding the extra-territorial application of the proposed UEM Bill, the Chairman considered that there would be enormous difficulties in enforcement.

72. Mr Allan DYER of HKCS highlighted the advantage of cryptographic technology. Instead of publishing the addresses, a list of cryptographic hashes of the addresses would be published. E-marketers could then apply the same hash function to the addresses on their mailing lists, and remove the addresses when the hashes matched. Mr DYER explained that because of the mathematical nature of a cryptographic hash, it was infeasible to derive the address from its hash. As such, the list could be freely published without providing spammers with a resource to misuse. Mr Lento YIP of HKISPA supported Mr DYER's idea and considered it worth-pursuing. He urged the Administration to consider employing the cryptographic hash function to protect the "do-not-call registers" from being abused. In this connection, the Chairman recapped his past suggestion to set up a "do-not-call register" for email addresses and notes that the Administration did not intend to set up such a register for the purpose of UEM Bill.

73. On concern about possible abuse of "do-not-call registers" listing valid telephone number, AD/Tel(S) explained that with the high penetration of telephone services in Hong Kong, the probability of connecting to a valid telephone number in random was very high. A spammer might be able to connect to half a million telephone numbers through random dialing of one million numbers within the number blocks already allocated by OFTA for the use of the telecommunications operators. Therefore, they might not need to resort to accessing the "do-not-call register" of telephone numbers in order to reach the recipients.

74. Ms Yvonne CHAI of HKISPA however pointed out that the "do-not-call registers" might be intentionally abused as a source of bona fide electronic addresses by spammers. She referred to the "national do-not-call registry" run by the US and recommended its adoption in Hong Kong. She said that to deal with inadvertent mistakes, telemarketers should be required to first register online with the "do-not-call registry" to give their identifying information to assist in future enforcement, set up their account to help trace what information they had accessed and keep good records to facilitate their own use. All telemarketers should also be

required to transmit their caller ID information.

75. AD/Tel(S) said that initially, three registers were proposed to be set up – one for telephone numbers for pre-recorded voice, sound, video or image messages, one for telephone numbers for Short Messaging Service/Multimedia Messaging Service messages, and one for telephone numbers for fax messages. An industry code of practice governing the operation of a "do-not-call register" for fax messages was actually in operation now. He nevertheless took note of deputations' view on "do-not-call registers" for consideration.

Admin

76. In reply to the Deputy Chairman on the information to be included in the published "do-not-call registers", AD/Tel(S) said that it would include telephone numbers and the effective dates on which such numbers would appear on the list. Dr P T HO of BCS(HK) was concerned about the validity of the telephone numbers in the "do-not-call registers" and whether they could have been maliciously included and without the knowledge of the user. In response, AD/Tel(S) said that the Administration would request the telecommunications operators to verify the identity of the person who had applied to place a telephone number onto the "do-not-call registers" so as to confirm that the person was the current user of that number. In this connection, the Chairman suggested that the Administration could seek the cooperation of telecommunications operators to include in their mobile phone service application form an option for users to join the "do-not-call registers".

77. In reply to Ms Emily LAU's enquiry, DSCIT(CT) confirmed that the "do-not-call registers" would apply only to the transmission of commercial UEMs. E-marketers should check against the "do-not-call registers" and delete the telephone numbers on the registers from their database before they sent out their commercial electronic messages.

78. On enforcement, members noted that the TA would issue an enforcement notice if he was of the opinion that an e-marketer had contravened the rules about sending commercial UEMs under the opt-out regime and "do-not-call registers". The e-marketer would commit an offence and be subject to penalty if he failed to comply with the enforcement notice. Ms Yvonne CHAI of HKISPA considered that the proposed two-tier enforcement mechanism ineffective because spammers might make use of the first-tier leeway where no prosecution could be taken out to commit an offence.

Accurate sender information

79. Noting that in implementing the proposed opt-out regime, the sender of commercial UEMs was required to include accurate sender information to enable a recipient to identify and contact the sender if necessary, Mr Jasper TSANG enquired how this could be implemented for UEMs using IVRS technology. He noticed that many machine-generated unsolicited marketing calls had been sent out without displaying the senders' telephone numbers. Mr TSANG was concerned whether the present proposal would require mandatory display of senders'

telephone numbers so that recipients could decide whether to answer the calls or not.

80. In response, AD/Tel(S) confirmed that the proposal to require the sender to include his accurate contact information was applicable to all forms of commercial UEMs, including voice telephony. The information should include the name, physical address and electronic address of the sender. If the sending party was an organization, the organization's name should also be included. AD/Tel(S) also confirmed that under the proposed Bill, senders of machine-generated unsolicited marketing calls must display their telephone numbers.

Small and Medium Enterprises (SMEs)

81. As the Deputy Chairman of the Business Facilitation Advisory Committee, Ms Emily LAU was keen to ensure that the proposed UEM Bill would not have an adverse impact on the operation of SMEs. She sought information on the estimated cost likely to be incurred for SMEs to meet the proposed legislative requirements.

82. In response, DSCIT(CT) reiterated that having regard to the need to provide SMEs and start-up enterprises in Hong Kong with room to promote their products or services using low cost means, the Administration had proposed to adopt an opt-out, rather than an opt-in, regime. Moreover, to allow time for SMEs to prepare themselves for compliance with the legislation, to set up the necessary system, gear up their equipment and train up their staff, it was the Administration's plan to commence different parts of the UEM Bill on different dates. On the estimated cost involved, DSCIT(CT) advised that according to the experience of New Zealand, it took a company about several thousand Hong Kong dollars to enhance the existing system to comply with the requirements under the proposed legislation.

Summing up

83. The Chairman thanked deputations' input and invited them to provide further views or raise further questions in writing, if necessary, for the consideration by Panel members. To facilitate meeting arrangements and presentation of views, the Chairman also reminded interested deputations' to register their attendance in advance.

Admin

84. The Chairman urged the Administration to take note of the views and suggestions expressed at the meeting, such as the use of cryptographic technology in publishing the "do-not-call registers" and the concerns about the effectiveness of the proposed enforcement regime based on the use of "enforcement notice", and to address these concerns when finalizing the UEM Bill.

VI Consultation paper on the establishment of the Communications Authority

CTB(CR)9/19/13(05)Pt.4 -- Legislative Council brief on consultation paper on the establishment of the Communications Authority

85. At the invitation of the Chairman, the Deputy Secretary for Commerce, Industry & Technology (Communications and Technology) gave a power point presentation on the Administration's Consultation Paper on the Establishment of the Communications Authority (published on 3 March 2006), which sought public views on the Government's proposal to merge the Broadcasting Authority (BA) and Telecommunications Authority (TA) into a unified regulator (i.e. the Communications Authority (CA)) for efficient, effective and co-ordinated regulation of a converging electronic communications sector. She highlighted the gist of the Administration's proposals as follows –

(a) The proposed CA would be tasked to promote the interests of consumers, ensure fair competition in the market and facilitate innovation and investment in the communications industry. As a unified regulatory body for the entire electronic communications sector, the CA would serve the interests of Hong Kong in an era of convergence and deregulation. Its public mission to promote competition and innovation also accorded with the protection of freedom of speech guaranteed under Article 27 of the Basic Law and the relevant provisions of the Hong Kong Bill of Rights Ordinance.

(b) A staged approach would be adopted under which the CA, upon its establishment, would continue to enforce the existing Broadcasting Ordinance (BO) and Telecommunications Ordinance (TO) and administer all the matters currently falling under the purview of the BA and TA. From there on, the CA would be tasked to review and rationalize the TO and BO together with the Administration. In particular, the separate competition regimes set out respectively under the BO and TO as well as consolidation of the competition provisions and the appeal mechanism on competition matters would be rationalized to ensure consistency and effectiveness in handling competition matters of the telecommunications and broadcasting sectors.

(c) The proposed CA would comprise seven members : a non-official Chairman, four non-official members and one official member appointed by the Chief Executive, and the Director-General of the executive department as the ex-officio member. The Office of the Telecommunications Authority (OFTA) and the Broadcasting Division of the Television and Entertainment Licensing Authority (TELA) would be amalgamated into a new government department

called the Office of the Communications Authority (OFCA), operating as a trading fund. Headed by a public officer ranked at D6 as the Director-General, the department would be the executive arm of the CA. The Administration did not anticipate that the proposed merger would give rise to forced redundancy of staff.

(d) Enabling legislation would be enacted to establish the CA, abolish the BA and TA, and repeal the Broadcasting Authority Ordinance (Cap.391) (BAO). The Administration planned to introduce a relevant Communications Bill into the Legislative Council (LegCo) by end 2006.

Resources requirements

86. Referring to the Administration's advice that the proposed merger of the BA and TA would not give rise to compulsory lay-off of staff, Mr Howard YOUNG remarked that there was expectation in the community that major merging and re-organization exercises would achieve better operational efficiency and more optimal use of resources, and hence resources savings. While appreciating that trade unions and employees' organizations were wary about re-organization and possible retrenchment, Mr YOUNG considered that the Administration should not abandon plans, if any, to achieve savings in manpower resources solely for the sake of avoiding staff redundancy.

87. In response, the Permanent Secretary for Commerce, Industry and Technology (Communications and Technology) (PSCIT) said that concrete resources requirements for the proposed CA were yet to be assessed and worked out. The manpower requirements would ultimately depend on the level of knowledge and expertise required to enable the CA to perform its coordinated regulatory functions effectively. He further explained that at present, the BA and TA were operating under different frameworks. The BA was a statutory body constituted under the BAO and funded by general revenue, while the TA was a public officer in charge of OFTA, which operated as a Trading Fund under the Trading Funds Ordinance (Cap. 430). With the merging of BA and TA to become the CA, one of the major challenges facing the CA was how to synergize the expertise and resources of the two regulators and put them to best use to achieve its mission and discharge its regulatory functions effectively. Amongst other measures to achieve the goal, enhanced training would be provided for existing staff to develop their professional skills. PSCIT said that notwithstanding the refined duties associated with a new dimension of work to be performed by the CA, the Administration had no pre-conceived plan to lay-off staff in connection with the establishment of the CA.

88. While agreeing that there should not be pre-conceived plans to reduce staff, Mr Howard YOUNG stated his view that efficiency initiatives to streamline operation and achieve savings should not be ruled out.

89. Noting Mr YOUNG's views, PSCIT advised that according to overseas experience involving the convergence of the regulation of the telecommunications and broadcasting sectors (such as the merging in the United Kingdom (UK) of five regulatory bodies into the Office of Communications (Ofcom) as the single regulator), there had in fact been an increase in the requirement for manpower resources, particularly staff with the requisite professional knowledge, in the initial one to two years of inception. However, savings could be achieved from the third year onwards.

90. In this connection, Ms Emily LAU cautioned that any new initiative which might have staffing implications should be proceeded with cautiously in order not to dampen staff morale. However, she shared the view that where there was room for more cost-effective use of resources, such as natural wastage of staff in which operational efficiency would not be adversely affected, the Administration should not hesitate to pursue such options.

Composition of the CA

91. Noting that the CA would comprise seven members, Ms Emily LAU said that the Administration should review whether such a lean structure would be sufficient for the CA to perform its regulatory functions effectively. She also suggested that the Administration should set out in the future Communications Bill the requisite eligibility criteria for appointment as unofficial members of the CA.

92. On the structure of the CA, PSCIT explained that a lean structure of seven members would ensure that views from different perspectives could be considered without compromising efficiency. With the proposed structure, the CA would be in a position to operate with greater transparency in its decision-making process and to respond to the aspirations of the community. Regarding the eligibility criteria for appointment, PSCIT said that due regard would be given to the capability and background of the individuals concerned. The Administration would take into account the feedbacks received during the public consultation exercise as well as finalization of the functions and responsibilities of the CA. For members' information, PSCIT advised that the Chairman of the UK Ofcom was a Lord and a university professor. In the case of the Federal Communications Commission (FCC) of the United States (US), all the five Commissioners were partisan political appointees.

93. In response to Ms Emily LAU's enquiry on the commitment expected of the unofficial members of the CA in performing their functions, PSCIT advised that the practices prevailing in comparable overseas regulators varied. In the case of the US FCC, all the Commissioners were full-time, albeit they were partisan appointees. In the case of the UK Ofcom, both its Chairman and Deputy Chairman had undertaken to spend three to four days per week in the work of Ofcom.

94. Ms Emily LAU stated her view that unofficial members, including the Chairman, of the CA should be remunerated at a level commensurate with the

requirements of their job. It would not serve the community any good if appointments were offered out of political considerations at a nominal remuneration. She emphasized that the appointments should be made objectively on the basis of merits and public acceptance, not in consideration of the political background or affiliation of the individuals.

Delineation of duties of Chairman and Director-General of the CA

95. Referring to the recent row between the top management and the Chairman of the Kowloon-Canton Railway Corporation (KCRC) which had aroused considerate public concern, Ms Emily LAU urged the Administration to take heed of the incident and delineate the powers and responsibilities of the future Chairman and Director-General of the CA in unequivocal terms. Referring to the ongoing scrutiny of the Securities and Futures (Amendment) Bill 2005, Ms LAU recapped that the Bills Committee would consider whether provisions should be added to the Bill requiring both the Chairman and the Chief Executive Officer of the Securities and Futures Commission to attend meetings of committees of LegCo to answer Members' questions, if requested. She added that such provisions were currently available under the Kowloon-Canton Railway Corporation Ordinance (Cap 372) and the Urban Renewal Authority Ordinance (Cap 563) and suggested that similar provisions should be included in the proposed Communications Bill.

96. In response, PSCIT advised that unlike KCRC, which was operating on prudent commercial principles, the proposed CA was a regulatory body and would be less complicated in terms of management structure. The future OFCA would be headed by a senior civil servant as its Director-General to provide executive support for the CA. PSCIT remarked that the Administration did not envisage any serious problem in rationalizing the delineation of roles and responsibilities of the non-executive Chairman of the CA and the executive Director-General.

97. The Chairman pointed out that the Bills Committee now scrutinizing the Securities and Futures (Amendment) Bill 2005 had raised concern over the proposed splitting of the chairmanship into the Chairman and the Chief Executive Officer posts, notably the proper division of role and responsibilities between the two, remunerations, conflict of interests and firewall arrangements, etc. He said that similar concerns would likely be raised in the study of the Communications Bill to be introduced and urged the Administration to give in-depth consideration to these concerns in advance.

Consultation

98. Ms Emily LAU recalled that the Administration had conducted a consultation forum in August 2005 in which representatives from overseas regulatory bodies including the UK and Australia had been invited to share their experience with the participants. She requested the Administration to provide a synopsis of the discussion for members' reference. She also considered that the Panel should invite deputations to give views on the Government's proposals at the appropriate time.

Admin

VII 2004 Digital 21 Strategy – Progress report for 2005 and targets for 2006

LC Paper No. CB(1)820/05-06(04) -- Information paper provided by Administration

99. The Assistant Government Chief Information Officer (Digital 21 Policy and Strategy) (AGCIO) gave a power point presentation on the progress made in 2005 in implementing the 2004 Digital 21 Strategy to drive the further development of ICT in Hong Kong, as well as the targets and action plans for 2006 and beyond. The key initiatives included –

(a) a pilot scheme to open up intellectual property in Government information technology (IT) systems and outsourcing of the Central Computer Centre;

(b) a sustainable e-government programme providing citizen-centric information and services;

(c) collaboration with the industry to promote infrastructure and business environment, including adoption of e-business, promotion of information security and tackling spamming, etc;

(d) institutional reviews including the proposed setting up of a unified regulator by merging the Broadcasting Authority and the Telecommunications Authority to provide a one-stop shop for resolving regulatory issues in a media convergent environment;

(e) support for technological development, particularly for the wireless and digital entertainment industries;

(f) development of a vibrant IT industry by promoting excellence, quality assurance and capacity building, and Mainland-related activities; and

(g) developing human resources in a knowledge economy.

100. AGCIO added that the Administration had started a new round of Digital 21 Strategy Review in the first quarter of 2006. It would come up with a draft document for internal consultation in mid-2006 and for public consultation in late 2006, and finalize the updated Strategy for promulgation in early 2007.

Research and Development (R&D) Centres

101. Mr Howard YOUNG asked about the scope of the five R&D Centres planned to be established by the Innovation and Technology Commission. In reply, AGCIO advised that the five R&D Centres were tasked to carry out R&D projects to cater for the needs and demands of different industries. Referring to

paragraph 28 of the Administration's paper, the Deputy Government Chief Information Officer (Planning & Strategy) highlighted that the five focus areas were (a) automotive parts and accessory systems; (b) logistics and supply chain management enabling technologies; (c) nanotechnology and advanced materials; (d) information and communications technologies; and (e) textiles and clothing. Members noted that the Panel on Commerce and Industry had discussed the new strategy for innovation and technology in Hong Kong.

Bridging the digital divide

102. On the initiative of bridging the digital divide, Ms Emily LAU considered that the Administration should take steps to ensure that knowledge and information on wider adoption of IT in the community would also be disseminated to persons with disabilities. In response, the Deputy Government Chief Information Officer (Operation) (DGCIO(O)) assured members that the Administration, in collaboration with the IT sector and non-governmental organizations, had been in close touch with concern groups for disabled persons to ascertain their need for IT support services and the problems they had encountered in the use of such services. These concern groups included, inter alia, those for visually impaired persons.

Admin 103. In this connection Ms Emily LAU requested the Administration to provide further information to the Panel in due course on the specific measures undertaken to assist persons with disabilities and disadvantaged groups in IT adoption.

Information security

104. Referring to the recent leakage on the Internet of the personal data of people who had made complaints to the IPCC, Ms Emily LAU asked what steps would be taken by the Administration to improve information security, particularly in government departments and public sector organizations.

105. In response, DGCIO(O) advised that the Administration was aware of the importance of information security protection and would continue to strengthen public education to promote public awareness of information security. The promotion activities included, inter alia, a series of publicity programmes, discussion forums, workshops and seminars etc for participation by members of the public, business associations and information security professionals. The estimated expenditure to promote information security targeted at the community in 2006-07 was $1 million.

106. Ms Emily LAU asked whether the Administration would, in the light of the incident in question, review its existing policy on outsourcing the development of computer systems involving databases of personal data information of members of the public. In response, DGCIO(O) advised that as far as outsourcing projects were concerned, the contractors engaged would only be responsible for developing the information systems concerned, such as writing computer programmes for data processing. Unless absolutely necessary, they would not be given access to the actual personal data. Moreover, stringent requirements were stipulated in the

contracts signed with the contractors requiring them to comply with provisions of the Personal Data (Privacy) Ordinance and the Government security regulations and guidelines, etc. The relevant service contracts also contained clauses on damages and penalties for breaches of contract terms.

107. Ms Emily LAU and Mr Albert CHENG recalled that according to the Chairman of IPCC during the earlier discussion on "information security", there were no provisions on information security requirements in the contract signed between IPCC and the contractor concerned. DGCIO(O) said that he was not in a position to comment as he did not have sight of the contract in question. To his understanding, the information system in IPCC was first set up in 1998 and a new system was installed in 2001. Hence, two separate contracts for IT service might be involved. DGCIO(O) confirmed that he had seen government tender documents and contracts containing express provisions on security-related requirements. He further advised that OGCIO provided advice on the technical aspects of a project which was the subject of a tender document, but not on the detailed content and drafting of the tender document for which there were standing guidelines on procurement. To assist departments in managing their systems, OGCIO had issued and circulated the relevant rules and guidelines on information security for reference of Government departments.

108. The Government Chief Information Officer supplemented that information security would continue to receive serious attention in the Digital 21 Strategy. He nevertheless reiterated that information security was very much a question of putting in place the right management framework. OGCIO would continue to assist bureaux and departments in strengthening their capability to manage the security of their information systems and deal with security incidents.

109. While agreeing that good management practices and an effective monitoring mechanism were important in enhancing information security, the Chairman considered that a clear message should be put across to all sectors, in particular various regulatory bodies which held a large database of personal data collected from members of the public.

VIII Any other business

The Deputy Chairman's proposal to visit Foshan to study the development of digital audio/multi-media broadcasting

LC Paper No. CB(1)1046/05-06(01)	-- Letter dated 24 February 2006 from Hon Albert Jinghan CHENG
LC Paper No. FS09/05-06	-- Fact sheet on "廣東省佛山電台數碼聲音廣播及數碼多媒體廣播" prepared by the Research and Library Services Division (Chinese version only)

110. Members noted the Deputy Chairman's letter dated 24 February 2006 to the Chairman stating his proposal and the Fact Sheet on "廣東省佛山電台數碼聲音廣播及數碼多媒體廣播" prepared by the Research and Library Services Division (RLSD). Members supported the proposed visit in principle.

111. Members also supported the Chairman's suggestion that if possible, the visit should also cover related development in IT in Guangdong Province. Members agreed that the Secretariat would explore the feasibility of arranging the visit with the Guangdong authorities.

Clerk

Overseas duty visit to Canada, United States and United Kingdom from 11 April to 21 April 2006)

112. In reply to members, The Clerk reported that details of the visit programme were being finalized. To facilitate exchange of views by the delegation and the overseas organizations to be visited, the Secretariat had prepared a concise fact sheet and a set of suggested questions in respect of each organization that the delegation would visit. The first batch of the papers had been issued to members on 13 March 2006. The RLSD aimed at completing the bulk of the research report by early April 2006.

113. Members agreed that the delegation would meet on 30 March 2006 at 4:30 pm to discuss the arrangements relating to the visit.

Date of next meeting

114. As he himself would be out of town on 10 April 2006, the Chairman sought members' view on whether the Deputy Chairman should be invited to chair the next meeting scheduled to be held on 10 April 2006, or whether the meeting should be re-scheduled. Members agreed to advance the meeting to 6 April 2006 at 10:45 am.

115. There being no other business, the meeting ended at 12:45 pm.

Council Business Division 1
Legislative Council Secretariat
4 May 2006