

立法會
Legislative Council

LC Paper No. CB(2)1655/16-17(04)

Ref : CB2/PL/CA

Panel on Constitutional Affairs

**Background brief prepared by the Legislative Council Secretariat
for the meeting on 19 June 2017**

**Report of the Task Force on Computer Theft Incident of
the Registration and Electoral Office**

Purpose

This paper summarizes previous discussion of the Panel on Constitutional Affairs ("the Panel") on the loss of the Registration and Electoral Office ("REO") notebook computers containing personal data of registered electors and follow-up measures.

Background

2. The Asia World-Expo ("AWE") was the fallback venue for the 2017 Chief Executive ("CE") Election. REO arranged for the setting up of the venue and testing of the computer systems at the AWE before the conduct of the election. According to the Administration, on 27 March 2017, i.e. the day following the 2017 CE Election, staff from REO went to AWE for packing and counting of the IT equipment at around 10:00 am. At around noon, the staff found that the two notebook computers stored in the concerned store room were missing and suspected that they were stolen. After repeated counting of the equipment, the REO staff reported the case to the Police at around 4:30 pm. On the same day, REO also reported the incident to the Office of the Privacy Commissioner for Personal Data ("PCPD") and the Government Information Security Incident Response Office.

Discussion held by the Panel

3. The Panel held a special meeting on 11 April 2017 to discuss the loss of the REO notebook computers containing personal data of registered electors and follow-up measures. Members were briefed of a summary of the incident and corresponding actions, as well as the result of a preliminary review conducted by REO. REO advised that it would work with relevant departments and comprehensively review the related arrangements on the collection, use,

processing and storing of the personal information of electors, system requirements and the overall security arrangements, etc., and would duly follow up on the recommendations to be made by PCPD upon the completion of its compliance check¹.

Preliminary review and improvement measures

4. Some members queried the need to take notebook computers containing the personal data of about 3.8 million geographical constituency ("GC") electors to the fallback venue at AWE as only 1 194 Election Committee ("EC") members were listed as electors for the 2017 CE Election. The Secretary for Constitutional and Mainland Affairs ("SCMA") and the Chief Electoral Officer of REO both advised that prior to the incident, they had no knowledge of the electors' information being brought to the fallback venue at AWE. REO advised that upon preliminary review of the practice, under the premises of protection of personal data and information technology ("IT") security, it considered that adopting the system developed for detainees for use in the Legislative Council and District Council elections for the CE Election was not appropriate as the bases of the electorate of these elections were different. In the future CE Election, the system would only store information of EC members.

Venue security

5. REO advised that there were altogether 32 computers in the store room concerned at AWE and six of them contained all electors' information. The two missing computers were placed on top of a carton. Some members pointed out that according to paragraphs 13.1 and 13.2 of the IT Security Guidelines of the Office of the Government Chief Information Officer ("OGCIO") regarding physical access and security measures, access record should be kept for audit purpose and arrangement should be made to lock up the computer equipment while not in use or after office hours. Members also asked about the manpower deployment in the fallback venue and the number of staff members who were authorized to enter the store room concerned.

6. REO advised that between 22 and 24 March 2017, there were about 20 non-IT staff members who were authorized to access the fallback venue but not the room storing the two computers. On the other hand, the room storing the two computers was used mainly by around 10 staff (including executive officer, electoral assistants, general assistants and IT staff). After the completion of setting up the venue and the testing of computers on 24 March 2017, REO staff left AWE in that evening, and notified the control room of AWE to deactivate

¹ Pursuant to section 38(b) of the Personal Data (Privacy) Ordinance, the Privacy Commissioner for Personal Data commenced an investigation on 10 April 2017 on the incident.

the card keys to the doors of the store room in which the notebook computers were stored, and turned the door into locked mode. REO advised that between 25 and 26 March 2017, no staff members entered the store room concerned but there were other staff members who went to AWE for other duties.

7. The standing CCTV cameras at various locations of AWE were directly connected to the AWE control room under round-the-clock surveillance by their security personnel. During the period between the commencement of setting up of the fallback venue to the moving out period after the election, REO had arranged for additional security supervisors and security guards to patrol and station at different positions of the venue. Some members expressed concern about the deactivation of the electronic lock which rendered it impracticable to trace the access record on the persons who had entered the room storing the computers.

Data security

8. Members in general expressed grave concern about the possibility of use of the personal data of registered electors for producing forged Hong Kong Identity Cards ("HKID"), or by fraudsters for conducting internet banking or phone-banking transactions. Members also urged the Administration to take measures against unauthorized changes of electors' registration particulars by a third party.

9. REO advised that:

- (a) the information of about 3.78 million GCs electors had been encrypted in accordance with the relevant security requirements and protected by multiple encryptions. The encryption algorithm used in the system conformed to the related guideline of OGCIO, and was one of the most stringent industrial standards in use;
- (b) REO had written to government departments and organizations of various sectors to notify them of the incident and appeal to their assistance in adopting appropriate measures to prevent criminals from using the relevant information as a means of identity theft in criminal activities;
- (c) following the PCPD's guidelines and advice, REO had informed all GC electors of the incident via emails or letters to raise their awareness and to minimize potential damage;
- (d) REO understood from the Hong Kong Monetary Authority that it had contacted a number of retail banks, which indicated that they

followed rigorous loan vetting and approval procedures. An individual could not obtain any bank loan or apply for credit cards by simply providing his name, HKID number and address. There were also corresponding additional security measures for online banking and telephone banking services, and high-risk transactions such as third party transfers were not allowed through telephone banking; and

- (e) REO encouraged electors to use the Online Voter Information Enquiry System to check their registration status and particulars. REO had reminded staff to watch out for any unusual or suspicious voter registration and change of particulars applications.

Accountability and internal investigation

10. Some members expressed concern whether any officials would be held accountable for the incident. The Administration advised that REO would conduct an internal investigation on relevant issues including the supervisory accountability. Should there be any evidence of breach of internal administrative codes or regulations by any staff members of REO, the Administration would take disciplinary action in accordance with the established procedures.

11. At the special meeting on 11 April 2017, SCMA also announced the setting up of a Task Force to conduct a comprehensive review of the causes and circumstances of the incident, and propose improvement measures on operational matters. The Task Force would submit a report to SCMA within two months.

Motions passed at the special meeting

12. The Panel passed two motions (in **Appendix I**) at the special meeting. The Administration's response to the two motions is in **Appendix II**.

Latest development

13. At the Council meeting of 31 May 2017, Dr Hon CHENG Chung-tai moved a motion seeking the appointment of a select committee and powers conferred by the Legislative Council (Powers and Privileges) Ordinance for the select committee to inquire into the incident and related matters. The motion was negatived.

14. On 12 June 2017, the Privacy Commissioner for Personal Data published the Investigation Report on the Loss of REO's Notebook Computers containing Personal Data of EC Members and Electors.

15. The Panel will discuss the Report of the Task Force and the Investigation Report on the Loss of REO's Notebook Computers containing Personal Data of EC Members and Electors at the next meeting on 19 June 2017.

Council Business Division 2
Legislative Council Secretariat
16 June 2017

立法會 CB(2)1200/16-17(01)號文件
LC Paper No. CB(2)1200/16-17(01)

政制事務委員會

在 2017 年 4 月 11 日的特別會議上

就議程第 I 項"選舉事務處遺失載有登記選民個人資料的
手提電腦事件及跟進措施"通過的議案

(議案中文措辭)

選舉事務處儲有全港登記選民個人資料的手提電腦失竊，是香港史上最嚴重的資料外洩事件。事件顯示選舉事務處對選民資料保安不足，未有採取所有合理及切實可行的步驟，導致近 378 萬地方選區選民的敏感個人資料被盜。鑑於事件影響範圍龐大，本委員會強烈譴責當局處理市民的個人資料時行政失當，並要求相關官員問責。本委員會促請政府制訂全面應變方案減低市民損失風險，包括驗證選民登記和更改的方法，重新檢視所有政府部門遵從政府資訊保安指引處理市民個人資料的做法，防止市民私隱外洩再次發生。

動議人：莫乃光議員

(English translation of the motion)

Panel on Constitutional Affairs

Motion passed under agenda item I

**"Loss of Registration and Electoral Office notebook computers
containing personal data of registered voters and follow-up measures"
at the special meeting on 11 April 2017**

The theft incident involving the notebook computers of the Registration and Electoral Office ("REO") containing the personal data of all registered voters in Hong Kong is the most serious data leakage incident that has ever happened in Hong Kong. The incident shows that REO has neither adopted adequate data security measures nor taken all reasonable and practicable steps to protect voters' information, resulting in the sensitive personal data of about 3.78 million geographical constituency voters being stolen. In view of the widespread implications of this incident, this Panel strongly condemns the authorities for maladministration in handling the personal data of members of the public, and requests that the relevant officials be held accountable for the incident. This Panel urges the Government to formulate comprehensive contingency plans to minimize the risk of loss suffered by members of the public, including conducting authentication of the applications for voter registration and change of voters' particulars, and reviewing afresh the compliance of all government departments with the Government's guidelines on information security in handling the personal data of members of the public to prevent the recurrence of privacy leakage incidents.

Moved by : Hon Charles Peter MOK

政制事務委員會

在 2017 年 4 月 11 日的特別會議上

**就議程第 I 項"選舉事務處遺失載有登記選民個人資料的
手提電腦事件及跟進措施"通過的議案**

(議案中文措辭)

選舉事務處遺失全港逾 300 萬選民資料事件影響嚴重，就此本會予以強烈譴責，並要求政制及內地事務局盡快公布選舉事務處的調查報告和懲處失職官員，以及提出補救措施，防止選民資料被非法使用，包括立即檢討有關更改選民資料的程序，確保得到資料者無法以任何方式更改任何選民的資料；同時，政府應檢視各部門處理市民個人資料的做法，就處理市民私隱方面，盡快制定相關的處理程序及加強加密級別，並制定針對不同事故下的應變方案。

動議人：黃定光議員

和議人：張國鈞議員
劉國勳議員

(English translation of the motion)

Panel on Constitutional Affairs

Motion passed under agenda item I

**"Loss of Registration and Electoral Office notebook computers
containing personal data of registered voters and follow-up measures"
at the special meeting on 11 April 2017**

In view of the grave implications of the incident in which the Registration and Electoral Office ("REO") lost the information of over three million voters in Hong Kong, this Panel expresses strong condemnation and requests the Constitutional and Mainland Affairs Bureau to expeditiously publicize REO's investigation report, penalize the officials concerned for dereliction of duty, and adopt remedial measures to prevent voters' particulars from being used illegally, including immediately reviewing the procedures for change of voters' particulars so as to ensure that those who have got access to such information cannot, in any manner, change the particulars of any voters; at the same time, the Government should review the practices adopted by various departments in handling the personal data of members of the public, expeditiously formulate the relevant procedures for handling issues relating to the privacy of members of the public with enhanced encryption grades, and put in place corresponding contingency plans to cater for different scenarios.

Moved by : Hon WONG Ting-kwong

Seconded by: Hon CHEUNG Kwok-kwan
Hon LAU Kwok-fan

政制及內地事務局
政府總部
香港添馬添美道2號
政府總部東翼



LC Paper No. CB(2)1390/16-17(01)

CONSTITUTIONAL AND MAINLAND AFFAIRS BUREAU
GOVERNMENT SECRETARIAT
EAST WING
CENTRAL GOVERNMENT OFFICES
2 TIM MEI AVENUE, TAMAR
HONG KONG

Our Ref.: CMAB C5/6/5
Your Ref.: CB2/PL/CA

Tel: 2810 2852
Fax: 2840 1976

11 May 2017

Ms Joanne Mak
Clerk to Panel on Constitutional Affairs
Legislative Council Secretariat
Legislative Council Complex
1 Legislative Council Road
Central, Hong Kong

Dear Ms Mak,

Suspected Theft of Notebook Computers of the Registration and Electoral Office

I refer to your letter dated 18 April 2017. Regarding the two motions passed at the Special Meeting of the Legislative Council Panel on Constitutional Affairs (“CA Panel”) held on 11 April 2017, our response is set out below.

The Constitutional and Mainland Affairs Bureau (“CMAB”) attaches great importance to the incident. The Police has classified the case as theft and initiated a criminal investigation. Upon receipt of the Registration and Electoral Office (“REO”)’s notification in the evening of 27 March of the suspected theft of the Office’s two notebook computers, the Constitutional and Mainland Affairs Bureau immediately instructed the REO to fully assist in the Police investigation. Furthermore, the Privacy Commissioner for Personal Data (“PCPD”) has also commenced a formal investigation on the case. Upon receipt of PCPD’s investigation report, the CMAB will instruct the REO to duly follow up and implement improvement measures recommended by the PCPD.

The REO also immediately reported the incident to the PCPD and the Government Information Security Incident Response Office. Following the advice of the PCPD, the REO has notified the affected electors, by letter or by email, of the incident to increase their awareness and ask them to contact the law enforcement agency where there are unusual circumstances, such as suspected theft of identity or personal data. The letter was uploaded onto the REO's website (www.reo.gov.hk) on 30 March. Meanwhile, the REO has also written to various business associations as well as relevant organisations of sectors including insurance, finance, banking, telecommunications, etc., to call for their vigilance and appeal to their or their members' assistance in adopting appropriate measures to protect the interest of their clients.

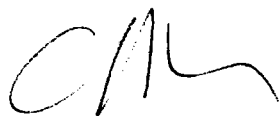
At the Special Meeting of the CA Panel held on 11 April 2017, the Secretary for Constitutional and Mainland Affairs ("SCMA") announced the setting up of a Task Force headed by a Deputy Secretary for Constitutional and Mainland Affairs, comprising representatives from relevant departments as members (including the Security Bureau, the Office of the Government Chief Information Officer and the REO). The Task Force will conduct a comprehensive review of the causes and circumstances of the incident and take into account the lessons learnt, and will propose improvement measures on operational matters in its report, including the handling of personal data, information technology security measures, overall venue security management, as well as the REO's internal supervisory structure and procedures, etc. The Task Force will submit a report and the relevant recommendations to SCMA within two months. After the Task Force has completed the report, we will give a proper account of the matter to the CA Panel.

As for disciplinary action, shall there be any evidence of breach of internal administration codes or any regulations by any member of staff of the REO, the REO will take disciplinary action in accordance with the established procedures.

Regarding the concerns raised by Members on the voter registration ("VR") system, particularly the change of voter particulars, we sought Members' views on the review of penalties and introduction of address proof requirement in relation to the VR system at the CA Panel meeting on 19 April 2017. Among other things, we have proposed to implement the address proof requirement on existing registered voters who apply for change of registered address first, and in the long run, we will extend the

requirement to cover new registration after the new measure has been implementing smoothly. The Electoral Affairs Commission will consider carefully views of the Members and introduce legislative proposals to amend the relevant subsidiary legislations in due course. We believe that after the introduction of address proof requirement in relation to change of registered particulars, the desire of a third party to impersonate a voter to submit application for change of registration particulars will be significantly reduced.

Yours sincerely,

A handwritten signature in black ink, appearing to be 'Ryan Chiu', written in a cursive style.

(Ryan CHIU)

for Secretary for Constitutional and Mainland Affairs

c.c. Chief Electoral Officer, Registration and Electoral Office