莫乃光
CHARLES MOK
立法會議員 (資訊科技界)
Legislative Councillor (IT)

立法會資訊科技及廣播事務委員會主席
葛珮帆議員

葛主席：

要求國泰航空公司就私隱外洩事件交代技術性問題

今次國泰航空公司私隱外洩事件嚴重，受影響的乘客人數多達約 940 萬。本人、業界及眾多市民關注為何國泰逾半年後才公佈事件，以及當初是否有遵守私隱條例，採取切實可行的步驟保障乘客個人資料。

據業界資訊系統專家指出，一般資料庫（Database）都會有查詢日誌（Query log）功能以記錄資料庫的作業活動，包括任何人讀取資料庫的記錄，以及讀取的資料內容等。事實上，如國泰的資料庫具備查詢日誌功能，今年三月發現系統出現的『可疑活動』的詳情以及乘客個人資料外洩的詳情應可於短時間予以收集，為何需要逾半年時間去了解和確認事件？

就此，本人要求國泰於 11 月 14 日立法會政制事務委員會、資訊科技及廣播事務委員會與保安事務委員會的聯席會議上交代有關資訊系統和資料庫管理上的一些技術性問題：

（一） 國泰表示於三月發現其資訊系統出現可疑活動後，五月確認乘客個人資料外洩，請告知（i）當初三月時是如何得知系統出現可疑活動，監察系統是以甚麼方式偵測可疑或入侵活動；（ii）可疑活動出現的時間以及資料庫/系統是否遭受持續攻擊，如是，受到攻擊的持續時間為何；（iii）及後五月又如何確認若干乘客個人資料外洩的詳情？

（二）早前，國泰給每一位受影響的乘客發出個人化的電郵，內容描述每一位乘客被不當取閱過的資料。請問國泰是否肯定，電郵描述以外的乘客資料沒有被不當取閱？

香港中區立法會道1號立法會綜合大樓917室
Room 917, Legislative Council Complex,
1 Legislative Council Road, Central, Hong Kong
2352 3129
3020 9867
charlesmok@charlesmok.hk
www.charlesmok.hk
Charles Mok 莫乃光
@charlesmok
CharlesMokOffice
Charles Mok

莫乃光
CHARLES MOK
立法會議員 (資訊科技界)
Legislative Councillor (IT)

（三）是否國泰所有資料庫均有查詢日誌功能（特別是今次受影響並管有乘客資料的資料庫/系統）；

（四）如國泰的資料庫/系統（包括今次受影響的資料庫/系統）有查詢日誌功能，是否有透過該功能調查有關駭客取閱乘客資料的詳情、乘客資料外洩的內容，以及國泰透過查詢日誌功能收集相關資料的時間；

（五）被入侵的資料庫/系統有否發現惡意軟件、木馬軟件、惡意載荷（Payload），如有，該等軟件的功能特徵為何？

（六）國泰有否訂立任何限制第三方服務供應商存取或連接資料庫/系統的政策？如有，詳情為何？

（七）國泰有否恆常進行進階持續性攻擊(Advanced persistent threat）之偵測和監察？

（八）國泰有否新措施防止類似事件再次發生，如有，請交代詳情。

莫乃光
立法會議員（資訊科技界）

2018 年 11 月 2 日

香港中區立法會道1號立法會綜合大樓917室
Room 917, Legislative Council Complex,
1 Legislative Council Road, Central, Hong Kong
2352 3129
3020 9867
charlesmok@charlesmok.hk
www.charlesmok.hk
Charles Mok 莫乃光
@charlesmok
CharlesMokOffice
Charles Mok