雲端運算與資訊保安

洩密、侵犯私隱及資訊保安事故頻生，轟動國際的維基洩密，25萬份美國政府絕密文件被揭露，令美國和各國蒙羞；最大社交網站Facebook被指不安全，有可能洩漏客戶資料；香港八達通被揭發出售約200萬名「日日賞」客戶的資料，獲利4,400萬元，香港市民咆吼，私隱專員和立法會也介入調查；這些事故令市民忐忑不安，筆者藉此分享一些觀點，讓大家多些思考。

發生這些事件，有多種原因：系統漏洞、程序問題、人為疏忽、惡意行為、利益引誘等，影響商譽、私隱條例、管治威信等，各方都誓言檢討及改善，堵塞漏洞，事件接踵而至，始終仍未能杜絕，更突顯了資訊系統在保安上的結構性問題。筆者不是保安專家，可用常理及淺易的角度探討資訊保安問題。

洩密和侵犯私隱不單在現今才發生，遠在互聯網時代之前都常有發生，相信自有人類以來就有。互聯網時代由上世紀九十年代開始，短短二十年，發展迅速，資料的傳送以接近光速來實施，95%的市民對新科技一知半解，就算天天在用，只知其言，而不知其所矣焉，將問題全部歸究現今的資訊科技，好像有點不公道。

水能載舟也能覆舟

每種科技都為人們帶來方便和價值，可能也有副作用，長江後浪推前浪，一去不復反。上世紀八十年代的傳真機，除了傳送文字，更可傳送圖像，但互聯網和電子郵件在上世紀九十年代興起，更快更便宜，重覆轉發都保持真跡，漸漸取代傳真機。擁有五億用戶的Facebook，其行政總裁Mark Zuckerberg揚言Facebook將取代電子郵件，因為電郵太慢。今年初，他曾說「隱私權的時代已經結束」。他的言行，會令有些人覺得震驚和失望。

儘管人人在大聲疾呼保障私隱，要求政府立法和加強執法，保護自己的秘密，但對他人的私隱及瘡疤，卻有濃厚興趣，千方百計去窺探和揭露。這正是針不拮到自己，怎知痛！在現實生活中， 2008年藝人艷照風波，報刊、雜誌、光碟和在網上流傳多時，很多人搜尋、下載和保存，直至警察拉人才收斂。近日流行的蘋果iPhone手提電話，機內有保護密碼，限制一些功能，但十居其九都被破解(Jail break)，這也侵犯了版權，政府有無執法？所以，不要「喊賊捉賊，五十步笑百步」。

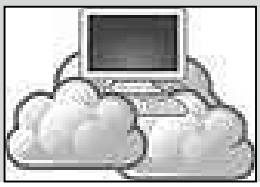
香港特首曾蔭權於2010年10月13日在立法會發表2010-11年的施政報告，勾劃出明年的施政方針。報告罕有地提到尖端資訊科技，例如：雲端運算和下一代互聯網等。自始，雲端運算成為熱門話題，這不是什麼嶄新科技，只是一個新名詞，將所有互聯網的應用，給予一個統稱，讓用戶更清晰，實際上，很多人天天都在使用雲端運算應用，例如：Hotmail，Gmail，MSN，Google doc，Facebook，Youtube等等。

雲端運算的五點特性

能稱得上雲端運算(Cloud Computing)的應用，美國National Institute of Standard and Technology定出以下五點雲端運算的基本特性：

1. 按需求自助服務 ── 用戶透過簡單介面，可自行設定自己的需要，例如：建立帳戶、重置密碼、修改設定等。
2. 互聯網上操作 ── 以任何標準器材（桌面電腦、手提電腦、上網本、手機、平板電腦），任何操作平台和瀏覽器，無需安裝軟件，在任何時間、地點、無拘無束使用。
3. 資源池 ── 將電腦資源（記憶體、硬碟儲存、運算功能等）集中後，再因應各客戶需要而分配。
4. 極度彈性 ── 功能的分配極度彈性，甚至自動，客戶可隨意增減。
5. 受控的服務 ── 雲端系統自動管理和優化各項資源，這些資源受到服務供應商及客戶的監管、控制和匯報。

依這些定義，Google的Gmail、Google



doc、Google App、Facebook、Youtube、eBay、微軟的Hotmail等都能符合。微軟提供的雲端平台Azure需安裝一系列的軟件才能開始，而將雲端應用局限於某台電腦，只可在微軟桌面操作系統運作，不符合美國的標準，難怪美國聯邦政府總務局及懷俄明州政府近日紛紛宣報棄用微軟，採用Google 的雲端服務。

有些人擔心，雲端運算將所有資料存在第三方手上，對資訊保安有疑問。有人也質疑，將資料存在自己公司內是否一定安全？在1950年代，很多人將辛辛苦苦賺來的錢，放在枕頭底，誰知石硤尾一場大火，將災民的血汗化為灰燼，後來大家將錢存入銀行，可從任何分行提存，方便可靠。相信有人曾遺失手提電話，失去金錢財物事小，最慘是失去朋友及客戶的聯絡電話、行事曆等，即使有備份，若你不是買同一款手機，備份也未必可以載入新手機，於事無補。現在很多款智能手機，有網上同步功能，將電話簿、行事曆等在網上備份，若然不幸失竊，只要出一台類似手機，按同步鍵，轉眼間將備份下載，這是雲端運算帶來的方便與優點遠比其顧慮多。

資訊保安可從多方面加強，使用者對電腦的認知太膚淺，往往貪圖方便而忽略安全，首先是電腦系統本身。桌面電腦的漏洞是結構性問題，為方便用戶，透過簡單程序便可隨意更改系統的設定，即使有密碼保護，都很容易破解，可防君子，卻阻不了駭客。我們上互聯網，是以TCP/IP的協定，透過65,536個連接埠(Port)將資料傳送，比喻為家裡的門窗，作業系統有65,536套門窗，全部打開，自由出入，方便傳送資料，方便自己之餘同時方便了駭客，成為資訊保安的隱患。若關掉所有門窗，正常的網上服務都不能運行。

防火牆有何用？

防火牆有兩大功能，除了有指定功能的連接埠，例如：80(瀏覽網頁)，110(電郵)等打開外，將其餘的連接埠關閉。另一功能是封包過濾，監察及限制透過連接埠的數據封包。加裝防火牆，好像萬無一失，聰明的駭客利用開通了的連接埠，透過必須的正常服務，並找出Outlook及IE的漏洞，利用Outlook的地址簿，向親朋好友發放有毒郵件，又向瀏覽器作出攻擊或盜取資料，防火牆形同虛設，所以資料洩漏，電腦病毒不斷擴散。

Linux擁有大型電腦系統的保安架構，比微軟安全，內置防火牆將不必要的連接埠關閉，若要開某些服務時，例如：採用SSL加密服務時，連接埠995會因應打開，關閉服務時，連接埠也相應關閉，方便又安全。Linux只容許Root才能安裝軟件及更改設定的權限，即使Linux系統被攻破或感染電腦病毒，只要將病毒刪除，重新開機，就不會將病毒擴散。

Android是採用Linux內核，近年被手機廠垂青，設計出近百款手機，功能多，款式多，價錢比iPhone便宜，並大行其道，銷量超越蘋果和微軟。各廠家再接再勵，今年將推出幾十款全新Android平板電腦，港幣兩三千元，媲美iPad，易用、方便、安全，是精明用家之福。

方便與保安的平衡

所有系統都沒有絕對的安全！在決定電腦系統時應要作出適當的取捨，究竟取其方便或安全呢？兩者要取得適當的平衡，若貪圖方便，可能面對嚴峻的資訊保安風險及嚴重損失。

很多國家的政府都擔心微軟封閉式系統及在保安上的結構未有全部公開，逐漸放棄使用，而轉用開放源碼軟件，既安全又方便，詳情可瀏覽http://www.linux.org/info/linux_govt.html。

簡錦源
香港Linux商會主席