資料私隱與數碼證書

電子商業（即透過網絡空間經營業務）正以急速的步伐發展。香港目前已有商業機構利用國際互聯網進行交易，例如萬國寶通銀行所提供的“網上理財”銀行服務，以及博學堂網上書店有限公司的“購物籃”網上購書服務。此外，香港政府亦決定約在2000年較後期間推行“公共服務電子化”計劃，在網上爲市民提供一星期七天，每天24小時服務。這些情況顯示愈來愈多本地公司會提供電子服務，以便與全球的趨勢看齊。

2. 當愈來愈多商業及政府機構透過電腦空間提供電子服務時，大量的個人資料便會透過電腦網絡而被資料使用者收集、儲存及傳送。以往保障私隱的有利條件，例如高成本、遠距離、不相容等因素，在目前的電腦網絡世界早已消弭於無形。

3. 電子商業備受關注的問題是如何建立消費者及經營者的信任和信心，而在信任和信心的各項受關注問題中，資料私隱已成爲最主要的考慮事項。

對資料私隱的關注

4. 在電子商業方面，大家對私隱問題表示關注，是當個人需要提供個人資料，例如姓名、地址、信用咭號碼等，作爲與業務夥伴在一個公開而無規管的網絡空間（例如國際互聯網）進行網上交易的一部分。這些關注主要包括兩方面。

(a) 對保安構成的威脅 這與保障在互聯網上傳輸的個人資料有關。除非已採取保安措施，否則資料在傳輸途中有可能被他人截取的危險。此外，資料亦往往在有關人士不知情的情況下有可能被修改。

(b) 對私隱的侵犯 這與冒認業務夥伴的身分而用不公平及不合法的方式收集個人資料，並且將有關資料用於詐騙或未經有關人士同意的非預期目的有關。事實上，不但他人可查閱我們在互聯網上傳送的資料，促銷者亦可爲了市場研究或直接促銷目的而有系統地發掘互聯網上的資料，藉以編製個人檔案及促銷名單。

保障資料私隱

5. 在香港，個人資料受到《個人資料（私隱）條例》的保障。顯而易見，條例的目的是要保障在世人士的個人資料私隱，但條例亦同時擔當了一項較少爲人週知，但卻同樣重要的任務，就是保障個人資料得以不受限制地從已實施資料保障法例的國家和地區自由流入香港，以保持香港經濟的持續增長。

6. 本港的機構屬香港的司法管轄範圍。基本的法律原則是*"在不使用電腦網絡的情況下屬違法的行爲在網上亦屬違法"*。故此，凡有人透過電腦空間進行詐騙，例如使用偷來的信用咭號碼在網上購物，或是設立網址欺騙市民大眾，根據香港的刑事法例，他們均會遭受檢控。

《電子交易條例草案》

7. 爲對香港的電子貿易作出應有的立法支援，政府草擬了《電子交易條例草案》，藉以確認電子記錄及數碼簽署的法定地位。香港郵政亦根據條例草案推出核證服務，管理及向本港的合法機構發出電子證書，以核實電子商業活動參與者的身分。

8. 根據香港郵政，每一電子證書用戶會有一對密碼匙——私人密碼匙(private key)及公開密碼匙(public key)。私人密碼匙是保密的，屬用戶私有。至於另一公開密碼匙則寄存於公眾目錄，供他人取用。送件者利用所持有的私人密碼匙用電子方式簽署訊息後，收件者要用送件者的公開密碼匙才可核實對方的簽署。香港郵政設立一項名爲公開密碼匙基礎建設（簡稱公匙基建）的密碼匙管理基本設施，負責管理及派發公開密碼匙及數碼證書。

潛在的私隱危機

9. 專家普遍認爲發展及使用核證機關及密碼匙加密科技，對推動安全可靠的電子交易至爲重要，這最終更會成爲參與電子商業活動必需具備的條件。公匙密碼加密法能解決數據完整及交易保密的問題，而電子證書則能進行核證及作出接達控制。

10. 雖然公匙基建方面的科技能對資料保安發揮積極作用，但公匙基建的使用亦隨之會對資料私隱構成威脅。以下是一些值得大家關注的事項。

(a) 公開密碼匙的目錄 核證機關的最重要功能是核實數碼證書中的公開密碼匙。數碼證書載有持有人的身分資料，例如核證密碼匙所需的姓名或身分證號碼。此外，數碼證書亦可能載有持有人的其他資料，例如性別或出生日期，而這些資料可讓資料持有人瀏覽接受數碼簽署代替密碼的某些網址內的特定內容。但是，數碼證書自動登載在核證機關的公眾目錄內，任何查閱目錄的人士皆可得悉證書的內容。除非採取特別措施保障當中一些較爲敏感的資料，例如個人的身分證號碼，上述讓公眾人士查閱證書內容的做法，可能引致個人資料被不必要地披露，甚至被濫用於非預期的其他目的。

(b) 密碼匙的還原 密碼加密技術可保障資料，令第三者難以擅自截取、偷聽或偷取。不過嚴格的加密法亦產生了一些附帶作用，令執法機構在目標人物不知情或未獲他們的協助下，更難查閱疑犯的已加密記錄內的資料。這種情況導致當局據理爭取制訂適用於政府的查閱規定，嘗試將密碼匙的還原與密碼匙的核證聯系起來，結果是出現一把“後門式”的機密密碼匙，令執法機構在毋須通知密碼匙持有人的情況下，可迅速查閱解密資訊。除非制訂具體的保安措施，限制查閱有關資料，以及規定只可在有理據的情況下方可使用上述還原功能，否則這種第三者可作合法查閱的做法，必定會引致更多私隱危機。

(c) 身分的追尋 荷蘭的密碼加密研究者最近發表了一份報告。報告的作者指出如不採取措施加強數碼證書的完整性，則*“我們每一個人大有可能被迫在一個遍佈電子監視工具的環境中與他人溝通及進行交易。”*這類關注源於大家可透過任何一張數碼證書來獨一無二地追尋收受證書者的身分，或查出內藏該證書的設施。故此，這些證書在系統內的流程是可以追查的，因而可用以編製個人交易資料檔案，以及與第三者的資訊連結或列成表格作對照之用，以達編製個人檔案的目的。

結論

11. 在電子交易環境下應用密碼加密技術可解決資料保安及保障的問題，即保

證交易資料不會被竄改（完整性），確實交易各方的身分（認證性）或作出法律上的承諾（不可推翻性）。不過，單獨使用密碼加密技術，並不足以解決不公平收集個人資料，或擅自將有關資料用於未經當事人同意的目的所引致的私隱保障問題。我們應致力加強電子交易資料的完整性，藉以同時配合資料保安及私隱方面的需要。

12. 故此，任何提供核證服務的機構，均應參照行之有效的私隱保障政策及指引，實施切實可行的私隱保障措施，以達小心保障用戶資料私隱的目的。這些政策應包括將所收集的個人資料限制在提供有關服務所需的範圍；規定所發表關於已發出的證書的資料，亦應只限於履行核實有關證書的有效期所需的資料，以及訂明就原本資料收集目的以外目的向第三者披露證書內的資料時所應遵守的規則。

個人資料私隱專員公署
一九九九年十一月