天下烏鴉一般黑——
如何平衡國家安全、個人私隱和通

前美國中情局員工斯諾登揭露美國國家安全局的「稜鏡計劃」（PRISM），至今下落未明，前途堪憂。但多得他冒險公開事實，在漣漪效應之下更多國家的同類計劃亦被揭發。英國通訊總部的「時態」（Tempora）行動和美國國安局的「恆星風」（Stellarwind）網絡監控行動是全球最強的互聯網情報收集計劃，而英國聯同美國、加拿大、澳洲和紐西蘭組成「五眼」（Five Eyes）的情報聯盟，其中英國對互聯網監控的規模最大。

各國政府收集和儲存大量來自全球的電話、電郵、互聯網瀏覽紀錄等通訊內容和能用以窺探溝通模式資料，網民的上網和通訊習慣和內容無所遁形，被儲存在某處的超級數據中心內。恐怕今次揭露的只是冰山一角，尚有龐大網絡監控機器不為人知。

今次 PRISM 事件揭密引發全球保護互聯網自由的討論固然重要，但亦令我百感交集。美國的行為固然偽善和可惡，該受譴責，但我亦擔心極權國家政府「以子之矛，攻子之盾」指責美國虛偽，作為變本加厲監控互聯網的藉口，試圖將秘密監控合理化、正常化。我一直關注和倡議言論自由和保障網上私隱，接受傳媒訪問時常被問到一個問題：在大數據時代，面對國家級的網絡監控，還有機會保障個人私隱和通訊自由嗎？我的答案是：不是不可能，但就必須靠我們自己了。

老大哥無處不在

有曰「誰控制了信息，誰就控制世界」，從古至今，政府都或多或少採取過監控公民的措施。網絡情報收集早是公開秘密，但一直秘密進行，一般網民無從知曉。今次的事件之所以轟動全球是因為他挺身而出指證美國無分國界持續有系統地監控網絡，要求主要互聯網服務供應商協助和直接從網絡骨幹（光纖電纜）蒐集通訊數據，將原本暗中進行的事暴露於全球目光之下。

憤怒過後，是時候應該思考在國家安全、個人私隱和通訊自由的各種矛盾中如何取捨和平衡。今天每個用戶手上的智能裝置，每日製作如相片、電郵等數據之外，亦令我們不斷在網上留下關於日常生活的痕跡（數碼影子）。有人說要了解一個人的想法，只要打開他的電腦或智能手機就一目了然。

令人擔憂的情況是，政府打著國家安全的旗號，以風險管理之名要求互聯網公司合作蒐集並分析普通公民的網上數據，為若公民知道自己網上一舉一動被全天候監視，可能會因為害怕成為監控對象而對網上行為自我審查，造成寒蟬效應，減弱監督政府和民主。

不可奉國家安全之名濫用科技

美國辯稱情報部門監督網絡遏止了恐怖威脅，挽救無數生命和保障國家安全。事實上，斯諾登事件後的民意調查結果表示，受訪的美國人對政府網上監控行為意見不一，但贊成政府網絡監控、認為斯諾登不應披露機密的人不是少數。可見，確有公眾接受政府使用網絡情報收集調查和制止恐怖活動。

我們都明白恐怖份子用精密的資訊科技策劃攻擊，國家採用資訊科技應對威脅無可厚非。但有兩點值得留意：

（1）國家安全和威脅的定義——
對民主政權來說，政府的責任是維護公共安全，阻止恐怖份子策劃大殺傷力攻擊或威脅重要基建。而專制政權監控網絡的目的是維持政權牢牢掌握在當權者手中，政府通過網絡蒐集資料監控思想和打壓異己。國家安全「威脅」的定義對於前者和後者已有天淵之別。

（2）對象、方法與效果——
針對有合理懷疑正籌劃恐怖活動或罪案的人收集通訊數據情有可原，但並沒有證據可以證實網上監控全世界能令世界更安全。大規模網絡監控是否真的能達到打擊罪案和恐怖活動的效果？再者，在國民知情下「依法」監察自己國民是一回事，在所有人不知情下把全世界包括外國人都監察是另一回事；美國連前者也沒做到（美國人也不知情），更遑論後者。

美國有評論指出，政府可能誇大大範圍監控網絡對反恐的成效，因為甚少成功阻止攻擊的案例是單憑網絡大規模監控取得線索，而不可以傳統的合法情報收集手法取代。

國家安全和公民權利並非完全對立

在全球化、複雜且不斷演變的科技環境中，平衡國家安全、私隱和資訊自由殊不容易，公眾的接受程度也和當時社會安全環境息息相關。我認為政府網絡情報收集應該在兩項前提下方可進行：

一、是以制度保障公眾知情權和嚴格監察公權力；政府不可用模糊或充滿灰色地帶的手法侵犯公民權利。政府應以合法、透明的原則使用網絡保護公民免受攻擊，並防止任何人藉漏洞濫權。政府應主動交代情報收集工作的用途和效果，而不是用途不明、秘密地收集大量數據。

二、是不可過份依賴和信任大企業。我們必須意識到互聯網公司儲存大量個人信息，大部份網絡數據流量都通過數十間大型互聯網公司，而他們的存在目的是盈利，向投資者負責。即使用戶的私隱和自由與國家法例要求有矛盾，它們亦有責任要和政府合作，開放自己的伺服器。因此，用戶關注政府行為的同時，亦應留意互聯網公司有否保障用戶權益，要求提高透明度，提防濫用資料作其他用途。

平衡國家安全和公民權利：制度、監督、問責

通過法律和技術手段，訂立適當的監控範圍和權限，防止網絡監控的無限擴展和濫用。

- 監控資料類型：只限元資料（通訊雙方的身份、地點、日期、時間等記錄），還是通訊內容（相片、影片、文件、電郵、聊天內容、瀏覽記錄等），收集所得資料能否識別個人身份
- 對象：鎖定於有嫌疑的恐怖或犯罪份子或是過度侵犯普通公民私隱，而且必須有合理懷疑，獲得清楚法院授權
- 用途：大規模數據採集和分析須符合國家與民眾的利益，例如用作反恐、反網絡黑客或網絡攻擊
- 賦予情報部門的權力：保存資料的時限，如何決定監視哪些資料，哪些資料需要額外授權
- 透明度：接受公眾、民意代表和獨立第三方審查，主動定期公開運作程序以及如何確保不被濫用

公民社會的角色：拒絕麻木，提高意識

見諸今次斯諾登事件，總有一天國家安全法會重臨，而互聯網及新聞自由必然首當其衝。若以國家安全為目的的網絡監控行為不受制度和公眾嚴格監督，很容易會被濫用作打壓政見的手段。

公民社會應該加強網上個人私隱保護的意識，更主動關注網絡上的私隱和資訊自由，尤其監察政府有否濫用制度漏洞逃避監督。我們要應該時刻保持警惕，連結不同持份者討論私隱和資訊自由事宜，認真參與政府諮詢和進行政策倡議。凡此種種都有賴傳媒，保障公眾知情權和協助市民理解和監督政府的行為。

對於政府為保障公共安全而必須進行的網絡監控，須持續、主動向政府施壓，要求政府清楚交代哪些人有權收集數據、數據類型、使用範圍和途徑，以及採取哪些措施來保護隱私權等。只有這樣，才可以在用戶權益、維護公眾安全、透明問責、機制監督之間尋求合理的平衡。

不少人會覺得，無論如何自己網上行為都被監控，既然自己的私隱沒什麼利用價值，便變得麻木、放棄採取任何保護措施。這想法大錯特錯。保護自己的數據和私隱，是我們每個網絡用戶不能推諉的責任，對經常接觸機密資料的記者來說更甚，由最基本的數據加密開始。

莫乃光
立法會議員（資訊科技界）