

從雲端運算探討政府、企業與個人的道德議題

博士生 李安國 教授 嚴奇峰

提 要

- 一、網際網路已成為現代大多數人的生活必需品，但在網路社會中，我們是否擁有跟現實社會中一樣的隱私權與人權？雲端運算企業Google的商業契約(服務條款)最令人爭議之處，在於Google沒有自我限定「在維修時才會存取使用者的資訊」。這讓Google被賦與更多的權利和操作空間，並可能將這些使用者的資訊作其它用途，如為商業獲利用的廣告，甚至侵犯使用者的個人隱私。
- 二、當雲端運算企業利用使用者對商業契約(服務條款)、法律條款等的不熟悉，試圖從其中謀取相關商業利益，已成為道德上的漏洞。而美國國家安全局前僱員Edward Snowden揭露的「稜鏡計畫」，更突顯出網路公司監控個人資訊隱私的重要性。
- 三、在雲端運算企業逐步走向大型化的趨勢下，倘若無適當的倫理規範或監督機制介入，以確保企業執行符合道德規範與使用者合理隱私的期待，是現今網路社會頗具爭議的議題。
- 四、本研究建議雲端運算企業應給予使用者合理隱私的期待，並以「硬碟即是城堡」概念對待使用者，即如同房東與房客之間的關係，尊重使用者的資訊。使用者自身更應在網路上掌握資訊自主，以避免任何風險。而身為軍人更是應當以保密為天職，從事網路相關活動時，更加注意資訊隱私的安全性。

前 言

現今社會，因為使用者常常需要在不同地點使用同一個檔案，造成檔案內容的不一致。雲端運算(cloud computing)、雲端服務(cloud service)的產生，透過網路普及的方便性，讓使用者從單一個人電腦的使用範圍，延伸到可以在任何地方使用。只需要透過網

路將檔案存在網路伺服器上(即雲端硬碟，(cloud storage))，由雲端運算方式提供相關的服務，如檔案存取、編輯、修改，文書應用…等，更重要是讓使用者能維持資料一致性，並能分享給其它使用者一起編修檔案、文件、內容等。

使用者在使用雲端運算(雲端服務)之前，需要閱讀與同意雲端運算企業的服務契

約(服務條款)。由於其服務契約(條款)的法律條款複雜性，以及使用者對於自身法律權益的認知與保護程度不一，往往造成使用者是否能充分理解其商業契約的各項細節，甚至是否有傷害自身的權益。但是，大多數人往往便宜行事，並能未詳加閱讀，以致直接同意該商業契約，提供使用於雲端運算的產品。使用者一個小小的同意動作，卻不知已經造成個人資訊大量的外洩，更代表自己主動喪失某些權益。

以知名的雲端運算企業Google的商業契約(服務條款)為例：¹

當您將內容上載、提交、儲存或傳送到「服務」，或在「服務」接收內容，或透過「服務」進行以上操作時，即表示您授予Google(及我們的合作夥伴)全球通用的授權，可使用、代管、儲存、重製、修改、製作衍生作品(例如翻譯、改編或變更您的內容，使其更加配合我們的「服務」)、傳播、發布、公開操作、公開展示與散布這類內容。您於本項授權授予的權利僅限用於營運、宣傳與改善「服務」，以及開發新的服務。即使您停止使用「服務」，本項授權仍持續具有效力(例如對您先前加到「Google地圖」之商家資訊的授權)。部分「服務」可讓您存取與移除先前提交至該「服務」的內容。此外，某些「服務」會有條款或設定縮限我們對提交至該類「服務」之內容的使用範圍。請確認

您擁有必要權利，可就您提交至「服務」的任何內容授予我們本項授權。

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.

可以發現爭議點在於Google有權在任何情況下，存取使用者所上傳的內容並做任何使用，而非自我限定「在維修時才會存取使用者的資訊」。²因此，Google已經被使用者

1 Google, Google Terms of Service, 詳參<http://www.google.com/intl/en/policies/terms/>, (2015), 檢索日期：2015年3月22日。

2 Quentin Hardy, The Lowdown on Google Drive, 詳參http://bits.blogs.nytimes.com/2012/04/24/the-lowdown-on-google-drive/?_r=0, (2012), 檢索日期：2015年4月24日。

授予可以用做任何用途的權利，包含採用使用者所上傳的內容，得以用作其商業利益。但對於使用者而言，洋洋灑灑的契約內容難以讓使用者迅速且明確瞭解其法律條款是否損及自身的權益。

2007年美國政府授權美國國家安全局(National Security Agent)以反恐行動為名，透過網路蒐集恐怖分子的資訊，稱之為「稜鏡計畫」(PRISM)。^{3、4}然而，其矛頭卻也直接或間接指向美國民眾，造成人民恐慌。從這「稜鏡計畫」與Google商業契約的關係來看，使用者授權給Google使用資料，而Google提供資料給美國政府來監控使用者，但使用者並不知情有此一行為。而且在法律上來說，因為使用者已同意Google的契約行為，就算使用者發現Google提供政府的行為已侵犯到個人隱私，但在法律上的訴訟仍難以成立。

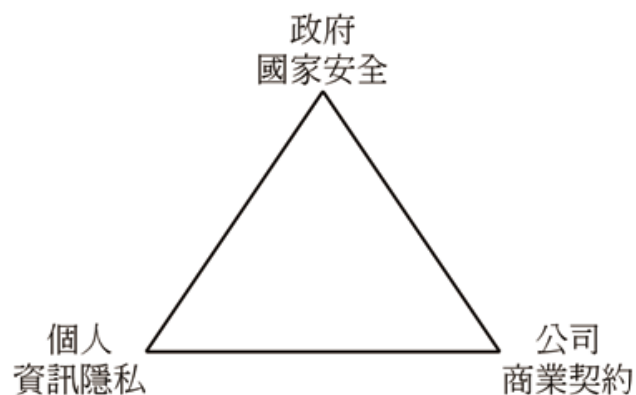
在市場自由經濟下，大公司將會大者衡大，雲端運算企業也將參與每個人的生活。但如果沒有適當的倫理規範或是管控機制，將讓大公司為了獲利而不擇手段，而讓使用者將成為生活與法律上的弱者。

因此，政府、公司、個人三者角色之間的關係，應如何取得平衡將是重要的道德

議題。本研究將先探討隱私權保護的歷史與法律發展，並透過政府的國家安全、公司的商業契約(服務條款)、個人的資訊隱私等三種觀點(如圖一)，分別兩兩探討彼此相互關係，並在結論中回歸到政府、公司、個人三者角色應有的做為。以期在現今的網路社會中，政府、公司、個人三者角色能夠取得適當的平衡點。

隱私權保護的發展

人與人之間的接觸日益頻繁，重視私人領域與保護也日益重要，該如何定義隱私權於個人與社會之間的界線？隱私權的分類又因不同對象得以區分多種。而今在網路社會的時代，個人資訊的隱私權將成為最嚴重的



圖一 研究架構

3 Barton Gellman and Laura Poitras, U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program, 詳參http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1, (2013), 檢索日期：2015年4月22日。

4 Glenn Greenwald and Ewen MacAskill, NSA Prism Program Taps in to User Data of Apple, Google and Others, 詳參<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>, (2013), 檢索日期：2015年4月22日。

問題。隨著科技發展與法律案件的探討，賦予不同程度認定保護隱私權的方式。

本章節將分別談討隱私權的定義，美國司法對隱私權的發展，以及個人對資訊隱私應如何面對與掌控自己的權益。

一、隱私權保護的歷史與法律發展

19世紀末，工業革命的興起，帶動攝影與新聞媒體業的出版。雖然強調新聞自由，但由於其方便性侵犯到個人生活品質，美國學者Samuel D. Warren 與Louis D. Brandeis共同發表的《The Right to Privacy》一文，認為人們有「生活的權益」(right to life)以及「獨處的權益」(the right to let alone)，⁵成為隱私權(privacy right)基本定義。也就是個人能保有不受外界干擾的權益，不論是因個人資訊保密，或是禁止新聞媒體業的公開與傳播，或是居家與私人領域不受他人無故進入等。並認為個人公開揭露的內容，應包含保護個人的「思想、情緒、敏感」或是「避免侵犯個人的權益」，此亦包含了侵犯隱私權的基本概念。

美國學者William L. Prosser基於美國學者Samuel D. Warren 與Louis D. Brandeis對隱私權的概念，進一步提出四種侵犯隱私權行為：

(1)入侵當事人的隱居或獨處，或他的

私事(Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs)。

(2)公開披露當事人令人尷尬的私人事實(Public disclosure of embarrassing private facts about the plaintiff)。

(3)公開宣傳讓公眾以錯誤眼光看待當事人(Publicity which places the plaintiff in a false light in the public eye)。

(4)利用當事人的姓名或肖像做為被告的優勢(Appropriation, for the defendant's advantage, of the plaintiff's name or likeness)。⁶

而這些成為日後法律參考的依據，也成為日後學者對於侵犯隱私權的觀點基礎。

聯合國在《世界人權宣言》(The Universal Declaration of Human Rights)，第12條關於隱私權的保護條文為：⁷

任何人的私人生活、家庭、住宅和通訊不得任意干涉，不得加以攻擊他的榮譽和名聲。每個人都有受法律保護的權益，不受這類干涉或攻擊。

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

5 Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol.4, No.5 (1890), pp.193-220.

6 William L. Prosser, "Privacy," California Law Review, Vol.48, No.3 (1960), pp.383-423.

7 United Nations, The Universal Declaration of Human Rights, 詳參<http://www.un.org/en/documents/udhr/>, (2015)，檢索日期：2015年3月25日。

透過此世界人權宣言，可以得知已包含適用於全球性的隱私權與侵犯隱私權的觀點，成為全世界認同的基本人權。

美國在殖民時期，由於英國政府常以搜索狀直接進入私人財產與住所進行無限制的搜查，造成民眾反彈極大，最終導致美國獨立。其中1792年訂定的美國憲法第四修正案(Fourth Amendment to the United States Constitution)限制政府不得恣意搜查私人財產與住所，此亦延伸為與個人隱私權相關：⁸

民眾的人身、住宅、文件和財產不受無理搜查和扣押的權利，不得任意侵犯。除依照合理根據，以宣誓或代誓宣言保證，並具體說明搜查地點和扣押的人或物品，否則不得發出搜查和扣押狀。

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

簡而言之，也就是「沒有搜索狀不得搜查和扣押」，以避免非法事情發生。此一關鍵點，成為日後法庭上，爭取個人隱私權的重要法律論點，也從此觀點延伸出許多隱私

權意義。

美國隱私權案例的保障範圍可以區分許多不同種類，其中與資訊隱私相關的是1928年的Olmstead v. United States(277 U.S. 438)案例，也是美國高等法院第一宗關於美國憲法如何保障資訊隱私的案例。當時由於聯邦探員未經法律允許而以電話監聽，並將其通訊內容做為法庭上的證物使用，違反被告的美國憲法第四修正案權益。當時，美國高等法院認為政府沒有實際進入當事人住所，並沒有違反美國憲法第四修正案，此保障政府可以搜索當事人的權益。⁹

後來上述法律論點，在1967年的Katz v. United States(389 U.S. 347, 353)案例被推翻。美國高等法院認為當時政府使用電子設備的行為監聽，雖然沒有進入被告的住所，卻能夠達到監聽的目的。因此，美國憲法第四修正案不只是限制政府非法搜索，同時也延伸對監聽行為的合法管制。其美國高等法院John Marshall Harlan II大法官也提出「合理隱私的期待」，認為「當事人已表現合理隱私的期待」(That the individual have a subjective expectation of privacy) 以及「此隱私的期待在社會中是合理的」(That the individual's expectation of privacy is “one that society is prepared to recognize as ‘reasonable’”), 以此二個準則認為美國憲法第四修正案主要是

8 Thomas K. Clancy, *The Fourth Amendment: Its History and Interpretation* (Durham, NC: Carolina Academic Press, 2008), pp.1-738.

9 Ming Li Wang, "Information Privacy in a Network Society: Decision Making Amidst Constant Change," *National Taiwan University Law Review*, Vol.5, No.1 (2010), pp.127-154.

「保護人，而非住所」。也就是說，住所並非做為判斷是否具有隱私權的唯一標準，而是以人為主。Katz v. United States (389 U.S. 347, 353) 案例開啟美國司法史對隱私權更明顯與合理的方向。

美國於1974年通過隱私法(Privacy Act)，規範政府未經同意不得洩露蒐集的個人訊息。1979年的Smith v. Maryland (442 U.S. 735)案例規範只要個人「自願公開」資訊，將沒有隱私侵犯的問題。此外，不同的法律規範適用於特定的隱私問題，如1970年公平信用報告法(the Fair Credit Reporting Act)、1986年電子通訊隱私法(the Electronic Communications Privacy Act)、1988年影像保護隱私權法(the Video Privacy Protection Act) 與1998年兒童網路保護隱私權法(the Children's Online Privacy Protection Act)等。

在美國司法史上，雖然美國對隱私權立場反覆，但其論點均在於如何界定政府與個人的界線，以及如何保護個人隱私的領域。總之，美國憲法保障個人基本隱私權以對抗政府過大的公權力，但目前美國相關的法律規範僅適用於特定領域的保護其隱私權。然

而在現今的網路時代，美國法律並未積極規定如何保護在網路、雲端運算中所蒐集與使用個人資訊。而傳統的法律條款僅適用於現實社會中，能不能充分保障網路使用者的權益，實在令人憂心。

二、掌控自己的資訊流向

雖然對於資訊隱私權有很多不同的定義，^{10、11}但其論點均著重在於「個人」與其「個人資訊」的緊密關係。這決定個人在社會生活中，用什麼樣的角色、資訊呈現、用什麼態度與其它人共處，以及延伸出哪些應該被尊重與保護的資訊。^{12、13}

保護隱私權可以分別從資訊隱私 (information privacy)與資訊自主權 (the right of information autonomy)二種角度討論。

1. 資訊隱私－從限制別人未經允許不得知道我們個人資訊，擴展到我們自己能控制個人使用與資訊流向。也就是說，我可以掌握自己的資訊，僅授權提供給我願意給的人，不得讓其它人可以從我願意給的人手中獲得，也就是二次使用。

2. 資訊自主權－因積極態度與消極態度的不同，而有不同的處理方式。

10 Joel R. Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?," Federal Communications Law Journal, Vol.44, (1992), pp.195-243.

11 Alan F. Westin, "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I - The Current Impact of Surveillance on Privacy," Columbia Law Review, Vol.66, No.6 (1966), pp.1003-1050.

12 Albert W. Alschuler, "Interpersonal Privacy and the Fourth Amendment," Northern Illinois University Law Review, Vol.4, (1983), pp.1-58.

13 Robert C. Post, "Rereading Warren and Brandeis: Privacy, Property and Appropriation," Western Reserve Law Review, Vol.41, (1991), pp.647-680.

(1)積極態度－自己能夠「控制個人資訊的權益」，並積極以立法方式保護個人資訊隱私的權益。

(2)消極態度－僅維持「獨處的權益」，任由當今法律的保護自己。¹⁴

現今，大多數的人則是以消極態度掌握自己的資訊流向，只有在自己親身感受到隱私被侵犯時，才會開始意識到自己的薄弱，而開始尋求法律協助。也因此，許多的法律都是在發生重大新聞、悲劇後，才會立法處理，屬於後知後覺。甚至，在其它國家發生的事，而在本國沒有發生，就不會認真看待，也就不會立法維護與處理。

然從資訊自主權強調隱私權，個人應該有權擁有與控制資訊流向，根據自由意識決定個人資訊的使用、保障個人身分定位與自我認同，避免不必要的外在環境影響，且可以選擇「獨處的權益」，不受任何隱私或私人領域的侵犯，最終保障個人基本尊嚴。

資訊科技的進步對保護個人資訊隱私造成很大的挑戰，所涉及的問題，不再只是誰擁有、保存這些資訊這麼簡單的問題而已，而是在於如何運用其資訊的問題，某種程度改變了個人與社會互動的方式，也就是個人在社會中如何呈現的方式。影響了每個人彼此之間的互動關係，個人與社會之間要用什麼觀點看待彼此。具體而言，對於個人資訊隱私的保護，在於如何面對網路社會，是否可以如同現實社會一樣的看法。但網路社會

屬於人類生活中的一部分，理應上應該與現實社會一樣，享有同樣的隱私權與人權。

然而與其追求法律的保護，更重要的是自己應該要有能力控制個人資訊流向，以維護資訊自主權。也就是在網路避免放上不必要的個人資訊，甚至私密照片、影音、檔案等。畢竟，就算網路、雲端運算企業沒有使用這些個人資訊，但是存放在網路上的伺服器，形同世界上任何人都可以去接觸。倘若有駭客破解密碼，取得這些資訊隱私，對個人也是傷害。

個人與公司的關係

網路拉近人與人之間的距離，也開啟與以往不同的全新世代與生活。在網路上，個人首先接觸網路、雲端運算企業提供的產品，像使用電信業者提供的上網服務，以及更進一步使用網路上的付費或免費產品，如使用Google搜尋引擎等，已讓個人與公司的關係從現實生活移轉到網路社會中。

當使用者在瀏覽網路時，所有行為可能已經被提供網路服務功能的公司蒐集起來，即使什麼都不做也是行為的一種。對網路、雲端運算企業而言，商業利益不單只是第一步從使用者收到費用，而是更進一步活用使用者所有的資訊，透過資料探勘(data mining)或大數據(big data)分析出更多的商業利益。

本章節從公司為了利益最大化而蒐集個人資訊，以及在網路社會中，個人使用公司

14 Charles Fried, "Privacy," Yale Law Journal, Vol.77, No.3 (1968), pp.475-493.

的產品會有合理隱私的期待，從個人與公司不同的角度進行探討。

一、公司蒐集個人的資訊經濟

起先網路只做為學術研究使用，由於使用者少，多半是學者與程式開發者使用，彼此多能自我約束。在網路大多是研究網路技術與發展，自然也沒有侵犯個人隱私權、資訊隱私權的問題。但自1990年代後，美國政府開放網路做為商業用途，商業網站迅速的增加。而當時蒐集個人資訊更不必得到許可，也不必通知使用者，便可以任意使用以提升商業利益，如販售給第三方。

網站獲取使用者資訊的方式，如要求填寫個人資訊，註冊成為網站會員才能使用該網站的服務。其填寫的個人資訊，如姓名、性別、生日、電話、地址、單位、職稱、電子郵件、興趣…等，已足以構成個人基本的資訊。

另外，網站Cookie技術的產生與運用，其原本目的是用以提升瀏覽網站的速度，透過儲存在瀏覽器的純文字記錄，可以下次登錄網站時，增快瀏覽網站的速度，如減少再次輸入使用者資訊、帳號、密碼等。這些網站Cookie存放在使用者電腦的硬碟裡，原本只能由被它產生的網站伺服器使用，¹⁵然而這項技術能夠讓使用者在不知情之下，輕易地讓網站獲取使用者的偏好資訊，包含使用者對哪些資訊有興趣，偏好什麼類型的新聞、

運動、媒體、議題、興趣等。

因此，透過使用者填寫的個人資訊，以及網站Cookie瀏覽網站歷史便足以瞭解一個人的生活資訊、偏好與興趣，長期累積足夠的資訊可以建立起使用者的側寫(profile)。透過使用者的側寫，就足以讓雲端運算企業建構起顧客在真實世界中的一面，或是只顯露於網路的一面。其側寫的資訊透過資料探勘或大數據的分析，將可以針對顧客的特殊屬性提供特定產品的銷售。

資訊科技對隱私權最大的衝擊在於改變公眾與私人的疆界，雲端運算企業蒐集使用者資訊帶來更高的效率，特別是有助於對特定顧客精確的銷售。因此，在大數據的時代，經濟利益取決於善用資訊結果。

然而，公司透過商業契約(服務條款)蒐集、使用個人資訊，也就是讓使用者以「自願市場行為」(voluntary market behavior)方式決定提供哪些個人資訊，或是決定何種程度的隱私保護。使用者能夠瞭解個人資訊是有經濟價值，並透過慎審的思考決定是否接受。因此基於此契約，在蒐集個人資訊前，理應上應該清楚告知使用者將使用什麼資訊科技以及做什麼目的使用。在此前提之下，使用者能有足夠的資訊與告知，以決定曝光哪些個人隱私。

但可以發現上述的契約模式是假設使用者充分瞭解其可能風險，而「自願地」提

15 Daniel Lin and Michael C. Loui, "Taking the Byte Out of Cookies: Privacy, Consent, and the Web," *Computers and Society*, Vol.98, No.Privacy (1998), pp.39-51.

供個人資訊。但很不幸的是，使用者可能都不是「自願地」提供個人資訊。因為，一旦拒絕提供個人資訊給特定網站，將無法使用存取該網站。也就是事實上，使用者沒有真正的選擇。如果未來出現在網路上，需要提供詳細個人資訊才能使用網路服務，將演變成「必要的邪惡」，而不是真正有選擇的自由。這種「自願地」同意，更像是「被迫自願地」同意。

而且，公司謹慎地小心擬定服務條款以保障公司的利益，但大多數使用者不會仔細閱讀與瞭解是否與自身的權益衝突，往往為了方便行事，而直接同意該服務條款。特別是品牌知名度越高，越會增加使用者對該公司的產品認同度（如Google利用大公司的知名度高，提供免費產品（Gmail、Drive、Chrome…等），但降低了使用者評估產品的影響，甚至忽略產品背後的風險。¹⁶一旦公司變更服務條款，將使用的資訊用在不是原本的目的，¹⁷可能不是使用者所樂見的。¹⁸

二、個人對公司有合理隱私的期待

雲端運算企業提供許多相關的雲端服務，如雲端硬碟允許使用者存放檔案。而當使用者在網路或雲端硬碟上使用密碼保護他們的資料是期待一種合理的隱私，這並不像公開在聊天室或布告欄發表一樣。¹⁹但是，如果用鎖（密碼）防止外人看到擁有者的內容，並且有權阻止其它人嘗試破壞或繞過「鎖」，則這「鎖」有助於擁有者建構合理隱私的期待。²⁰因此，美國憲法第四修正案應從「家是城堡」（house is castle）的概念延伸成「硬碟是城堡」（storage is castle），將這概念類比於雲端運算企業與使用者的關係，如同屋主與房客的關係，而不是單純訊息交易的商業關係。因此，屋主擁有鑰匙，並不表示屋主可以隨意進入或移動房客的東西給其它人，甚至商業用途。將資料儲存在網路、雲端硬碟的使用者對提供雲端服務有合理隱私的期待，而雲端運算企業也應用相同價值觀對待使用者。²¹

個人資訊隱私就像器官交易一樣，往往成為高度爭議問題，不能等閒視之。學者

16 Philip Kotler and Kevin Lane Keller, *Marketing Management* (Upper Saddle River, NJ: Prentice Hall, 2012), pp.482.

17 Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," *Southern California Law Review*, Vol.75, (2002), pp.1083-1113.

18 Shaun B. Spencer, "Reasonable Expectations and the Erosion of Privacy," *San Diego Law Review*, Vol.39, No.3 (2002), pp.843.

19 Matthew J. Hodge, "The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com," *Southern Illinois University Law Journal*, Vol.31, (2006), pp.95-122.

20 Orin S. Kerr, "The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?," *Connecticut Law Review*, Vol.33, No.2 (2001), pp.503-533.

21 Ching Yi Liu, "Cloud Computing Internet Privacy," *Taiwan Bar Journal*, Vol.14, No.2 (2010), pp.39-52.

Daniel J. Solove列出在大數據時代，四種隱私侵犯資料的型式：(1)訊息蒐集 (information collection)，(2)訊息處理 (information processing)，(3) 訊息傳播 (information dissemination)，以及(4)入侵 (invasion)等。²²指出網路資訊隱私應該嚴肅重視，因為當網路被蒐集的資訊經二次處理與分析，可以產生驚人的經濟效益。科技的發展帶來人們資訊傳送與創新的方便，但相對的，對個人資訊隱私的侵害將日益嚴重，²³甚至偽造個人使用記錄或不當言行，對使用者的傷害將難以彌補。

三、道德規範與清楚的風險告知

在法律上而言，個人相對於公司明顯是弱勢，應當有道德規範或法律明確禁止蒐集個人資訊做為其它用途。儘管公司在商業契約 (服務條款) 中，有註明所上傳的個人資訊將作為其它用途等模糊帶過，可是其包含範圍很大，而且未明確說明實際用途，如用於商業利益或是提供政府監控。

當然，個人可以自願選擇成為第三方資料或廣告對象處理模式，但畢竟是少數的人。因此，更需要建構個人資訊保護隱私權的方向，對大多數人而言，會希望個人資訊是有保護，也就是合理隱私的期待。

在網路社會中，無論使用者是否自願，應如同在現實生活享有同樣的個人權利，也

就是合理隱私的期待。因此在契約中，公司應提供明確的文字讓使用者能夠短時間輕易瞭解個人權益。

然而，這又如同香菸盒所標示的「吸菸有害健康」，保險理財廣告所標示的「投資一定有風險，基金投資有賺有賠，申購前應詳閱公開說明書」，到頭來仍需詳細閱讀說明書。但目前雲端運算企業的契約上，並沒有這類簡短的風險說明「本公司會將使用您所上傳的資訊做商業用途」。換言之，對大部分的人而言，其實並不知道雲端運算企業會將個人資訊做商業用途的風險。

無論是否菸盒或是保險理財廣告的警語，都是漫長累積的危害健康與理財不當問題造成嚴重的社會議題，最後促成政府要求公司配合，以逐步減少風險。然而，對於生存在網路時代的人，網路生活已經成為生活必需品，但是每個人對於自己的權益並沒有深度重視，最主要是目前沒有相關的重大社會議題上過新聞，自然沒有社會輿論施壓，也讓雲端運算企業可以恣意的蒐集使用者資訊，做任何的商業用途。

道德規範如同社會文化一樣，需要長時間的醞釀與影響，民眾才会有共識。對使用者而言，無論在現實社會中「人」的身分，或是網路社會「使用者」身分，同樣都希望有合理隱私的期待，也應當有相同的人權與

22 Daniel J. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review, Vol.154, No.3 (2006), pp.477-560.

23 Lawrence M. Friedman, "The Eye that Never Sleeps: Privacy and Law in the Internet Era," Tulsa Law Review, Vol.40, No.4 (2004), pp.561-578.

隱私權。

公司與政府的關係

社會用什麼樣的經濟形式對人民是最好的？放任市場機制決定？還是由政府介入市場，介入到什麼程度？一直是經濟學家爭論不休的問題。強調資本主義至上，或是國家資本主義，在全世界都有成功的案例，也都有失敗的案例。

美國自從1776年建國獨立以來，一直強調市場經濟與放任自由競爭，由於過往受到英國殖民時期的影響，美國政府便傾向維持在有限、小政府的模式。因此，大部分議題都是自我規範或是市場機制來解決問題，非不得已，政府絕不會插手介入。

本章節從美國以資本主義為主的國家，認為公司應由市場機制來決定生存與自我規範，以及政府雖然放任市場自由競爭，卻又以國家安全名義要求公司配合的角度，來探討公司與政府之間的關係。

一、公司由市場機制來自我規範

由於美國強調資本主義的國家，相信小而美的政府對大家是好的，因此，政府對市場經濟的拿捏一直維持某種程度的放任。

經濟學家相信市場透過看不見的手 (invisible hand) 來調節 (也就是民眾的消費影響)，政府倘若介入市場，將如同絆腳石一樣，對市場造成某種程度的傷害，這雙強而

有力的手 (heavy hand) 將會傷害自由競爭和創新。此外，因為市場導向，自然強調“由下而上”成為規範，也就是不論規範如何，都是民間的影響去改變公司的走向。也就是說，透過網路的自我規範來管理問題，政府不應「由上而下」的介入。²⁴然而，市場自我規範真的可以實踐，還是純粹是理性的狀態？

政府降低對市場的管制，公司將能提供市場更好的服務與更有效率。然而，若市場經濟的濫用過大，也就是公司透過商業契約 (服務條款) 剝奪使用者的權益，政府則需要介入市場以限制公司的活動，或者透過法律修正成合理的商業契約 (服務條款) 以保障民眾的權益，或民眾集體抵制公司非法濫用經濟能力。

自從1980年代，國際組織對於個人資料或資訊隱私的保護，達到相當程度的共識。雖然美國基本上同意經濟合作暨發展組織 (Organization for Economic Co-Operation and Development, OECD) 的提議，但是目前為止並沒有透過立法來通用保障任何個人資料的標準，而是針對特定對象的資訊個別立法保護隱私權。一般來說，美國在通訊組織中對個人資訊的隱私使用，傾向鼓勵產業自我規範的態度，甚至電子商務市場也是同樣的立場。²⁵

然而，如果期待產業或公司對資訊隱

24 Paul M. Schwartz, "Internet Privacy and the State," Connecticut Law Review, Vol.32, (1999), pp.815-859.

25 William J. Clinton and Albert Gore, Jr., A Framework for Global Electronic Commerce, 詳參<http://www.w3.org/TR/NOTE-framework-970706>, (1997), 檢索日期：2015年4月10日。

私自我規範，仍是需要時間的考驗。產業自我規範乃是受到市場機制的影響，然而，市場機制失靈的話，對於公司的自我規範更無影響。尤其是現在所有的一切聯絡都是透過通訊、網路來聯繫。所有的資訊其實都曝露在大公司的監控之下，也如同極權體制一般。另外，將保護個人資訊隱私交由市場機制處理，可能導致市場失靈。因為市場機制只有在公開透明的情況下才能有效運作，也就是，個人需要能夠確認是誰在蒐集使用個人資訊。但是對蒐集資訊的雲端運算企業而言，往往利用商業契約（服務條款）、法律條款來模糊此一議題，而非充分透明且清楚，導致個人無法真的明瞭自己的個人資訊隱私權是否被侵犯，造成市場機制失靈。也因此，將個人資訊蒐集的透明化，與公司所追求的利潤最大化相比較，所能獲取的商業利益是十分可觀。因此，期待公司自我規範，其實難以符合保護資訊隱私的原則。

因此，在Google的商業契約中，縱使對使用者有風險，但是政府傾向由市場決定，也就是使用者自然淘汰公司與產品。然而，對大多數的使用者而言，往往不會詳細閱讀其服務條款，甚至並未充分瞭解是否與自身的權益衝突。因此，想要透過市場自然淘

汰，並不容易，只能透過業者自身道德規範或是政府立法來處理。

二、政府以國家安全為名進行監控

自從2001年的911恐怖攻擊事件發生後，美國政府提升國土安全的層級，也更加著重先發制人的戰略思考，如對外發動的阿富汗、第二次伊拉克戰爭等，對內則是對恐怖分子的監聽。「稜鏡計畫」是非法智慧型監控程式，是國家安全局透過主要的網路公司蒐集海外人士的網路通訊，以監控使用者的活動（包含電子郵件、檔案、聊天和搜尋記錄）。「稜鏡計畫」的前身即是時任美國總統的George Walker Bush簽署恐怖分子監聽計畫（Terrorist Surveillance Program），當時曾遭遇廣泛批評，其計畫的合法性亦未經過海外情報監聽法庭（Foreign Intelligence Surveillance Court, FISC）核准而受到質疑。²⁶但之後有同樣性質的「稜鏡計畫」卻得到海外情報監聽法庭的授權，且在接任的Barack Obama總統任內，仍然持續運作，縱使Barack Obama總統在當選前曾大力抨擊當時George Walker Bush總統的監聽不合理。²⁷

在2007與2008年間，美國政府曾威脅Yahoo，如果Yahoo沒有遵照國家安全局的「稜鏡計畫」要求提供使用者資料，Yahoo

26 John W. Dean, George W. Bush as the New Richard M. Nixon: Both Wiretapped Illegally, and Impeachably; Both Claimed That a President May Violate Congress' Laws to Protect National Security, 詳參<http://writ.corporate.findlaw.com/dean/20051230.html>, (2005), 檢索日期：2015年4月29日。

27 Glenn Greenwald and Ewen MacAskill, NSA Prism Program Taps in to User Data of Apple, Google and Others, 詳參<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>, (2013), 檢索日期：2015年4月22日。

將會每天收到250,000美元的行政處罰。縱使Yahoo堅持此種行為違憲而拒絕參與，但是美國政府仍控告Yahoo，並在海外情報監聽法庭秘密聽證。不幸的是，Yahoo輸掉官司。最終Yahoo被迫成為提供「稜鏡計畫」使用者資訊的公司之一。²⁸

目前已知，至少9家網路、雲端運算企業Microsoft(2007年)、Yahoo(2008年)、Google(2009年)、Facebook(2009年)、PalTalk(2009年)、YouTube(2010年)、Skype(2011年)、AOL(2011年)和Apple(2012年)陸續主動或被迫參與「稜鏡計畫」，而據傳Dropbox(2012年)也被迫參與。^{29、30}雖然這些網路、雲端運算企業是否是被動加入或是如Yahoo一樣曾經堅持立場，但都有公開發出新聞稿說明拒絕或沒有參加「稜鏡計畫」。³¹巧妙的是，這些新聞稿的說明用字譴詞都是十分小心，並且

沒有排除國家安全局以反恐名義、國家安全為由蒐集資料的任何可能性。³²

而從這些網路、雲端運算企業推出產品的高使用率(如電子郵件、搜尋引擎、社群網站、影音網站…等)，可以看出已經幾乎覆蓋全國，甚至全球會上網的民眾。也因此，如何篩選出恐怖分子與美國民眾，是一件極具挑戰的事。

美國政府為了監控海外恐怖分子，透過主要網路、雲端運算企業以系統化與大量偵察存取追蹤可疑的恐怖分子、嫌疑犯可能涉嫌的恐怖活動。縱使法律授權監控特定對象，但仍有意或無意地、直接或間接地擴散到其它的美國民眾，等同於槍口轉向開始秘密蒐集自家美國民眾的資訊與分析。³³

正如英國小說作家George Orwell在《1984》一書所描述「老大哥正在看著你」

28 Yahoo, Shedding Light on the Foreign Intelligence Surveillance Court (FISC): Court Findings from Our 2007-2008 Case, 詳參<http://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence>, (2014), 檢索日期: 2015年4月10日。

29 Barton Gellman and Laura Poitras, U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program, 詳參http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1, (2013), 檢索日期: 2015年4月22日。

30 Glenn Greenwald and Ewen MacAskill, NSA Prism Program Taps in to User Data of Apple, Google and Others, 詳參<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>, (2013), 檢索日期: 2015年4月22日。

31 Frederic Lardinois, Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL and Apple Deny Participation in NSA PRISM Surveillance Program, 詳參<http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/>, (2013), 檢索日期: 2015年4月10日。

32 Michael Liedtke, Denials in Surveillance Program Require Decoding, 詳參<http://news.yahoo.com/denials-surveillance-program-require-decoding-000528228.html>, (2013), 檢索日期: 2015年4月30日。

33 Laura Poitras and Glenn Greenwald, NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video, 詳參<http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>, (2013), 檢索日期: 2015年4月12日。

(big brother is watching you)的情節。³⁴在過去，只有極權或威權政府才會對所有人民或是異議分子進行監控。然而，如今在民主國家也發生同樣的事情，並不侷限於恐怖分子、已經犯罪或即將犯罪的嫌疑犯等特定對象，而是將所有人列為可疑對象監控，只要使用網路就已成監控對象，並要求雲端運算企業主動或被動地配合提供電子郵件、瀏覽記錄、聊天記錄等行為。這種行為，名義上的民主政府，其實已跟極權或威權政府無異。

三、愛國情操的拿捏

美國是崇尚資本主義的國家，自由放任市場經濟決定一切，但是政府卻以國家安全為名監控民眾。不難令人想到美蘇之間的冷戰時代，美國社會因為敵對方共產黨的存在，擔心被蘇聯赤化而產生恐懼共產主義的現象，麥卡錫主義(McCarthyism)的產生即是在這種恐共風潮下產生的政治迫害運動。透過激發人民的愛國情操，在社會引起廣大的風暴。雖然，現在美國是反恐行動，但同樣都是激發人民對國家的愛國熱誠，保衛自家國土安全，容易在政客鼓動、濫情、狂熱的情緒下，誘發人民逐步放棄民眾的自由與權益。甚至透過新聞媒體，對人民左右其思想，引誘人們激起愛國熱誠。

因此，需要理性、客觀地看待如何實踐國家安全，尤其在現今資訊充沛的時代。憲法捍衛個人自由，限制政府濫用權力。如果

政府已經侵犯了民眾最基本的權益，如隱私權，同時也阻礙了Edward Snowden的言論自由，更遑論企業為謀取商業利益的行為。政府和企業需要重新規範自己的行為，以道德規範自我規範做為最高標準，才能讓相對弱勢的民眾能夠放心。

政府與個人的關係

不同人對於同一件事，因為不同的角度，即有不同的道德觀點，所判斷的結果也不盡相同。造成差異的原因，是因個人的立場不同，所用的道德標準即不同，判斷他人的道德標準，甚至對自己所採取的道德標準，在不同的情境下也會有所不同。如同在網路世界中，有些人自認是正義魔人，高舉言論恣意批評現實世界事件的不滿，但在現實生活中，卻可能會接受自己去做了自己在網路所批評的事。網路的隱匿性，讓人得以在網路社會與現實社會用不同的身分生活。每個人追求道德的理想境界不同，有些人可以某些情境下的道德不完美，選擇安身立命，多一事不如少一事；有些人追求極致的道德完美，近乎道德潔癖的程度。

本章節分別從個人的道德論、政府的目的論來做一談討，並且談討在道德論與目的論的天平兩端之下，資訊隱私應立於什麼樣的平衡點。

一、個人的道德論

德國學者Immanuel Kant提出道德論

34 George Orwell, Nineteen Eighty-Four (London, UK: Secker and Warburg, 1949), pp.1-267.

(deontology)，崇尚對人性的尊重，認為人權是普世價值。人有自尊，因為人是理性且獨立的動物，有選擇的自由與行動。善意的道德價值是指義務做好的行事動機。只要違反義務做好的行為，即使對大多數人有利，但仍是道德的。

Kant提出定然律(Categorical Imperative)中的第二個定律：³⁵

你對待人的方式，無論你自己身為人，或是其它任何人，從不做為手段。

Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end.

因為每個人都是個人自由，如果將他人當成工具，就不是把人視為“人”。

在美國政府的監控中，為了「國家安全」的目的，甚至是無辜的民眾、公私立的機構與單位都將被牽連。所有受影響的使用者已然成為其系統工具，因為他們被視為使用者，而不是「國家安全」中的「民眾」。民眾是整體、抽象的「群體」，而使用者是特定的個體。所以，在美國政府的眼中，網路使用者對系統而言只是工具、無情感的物品。因此，站在Kant道德論的倫理觀點，無論「國家安全」具有多崇高的價值，只要美國監控沒有把使用者視為「人」就是錯誤的。

而個人道德標準，往往只問己身的善惡與喜好，而不從結果、他人規則、社會規範做為基礎來決定道德。人的判斷是非能力，是順從內心的感覺。從「稜鏡計畫」的洩密者而言，是基於什麼動機而洩密？Edward Snowden自稱不是叛徒，也不是英雄，而是認為美國政府不應該侵犯美國，乃至全球上網的使用者的隱私。對於大多數人而言，911恐怖事件已經十分遙遠，但是為了國土安全，而喪失多數人珍貴的自由，這不是民主國家應有的面貌。

Edward Snowden揭露「稜鏡計畫」的資訊，本身已違反職業倫理，尤其是在執行國家安全任務的，其言論自由和行為應受職業規範。違法者固然有犯罪事實，但其工作內容必須合乎憲法的法律規範。也因此，在不同的政治理念下，Edward Snowden選擇以合乎大眾的權益，以非法的方式對抗政府不合理的行為。

二、政府的目的論

英國學者Jeremy Bentham認為道德的最高原則是幸福最大化，也就是追求幸福扣除痛苦後的總和最大化，只要能夠將幸福最大化的方式都是正確的。所以，不論行為的動機為何，而是著重行為過後的結果。只要對大多數人有利，那這行為就是對的，此即為目的論 (teleology)，亦稱之為功利主義 (Utilitarianism)。³⁶

35 Immanuel Kant, Groundwork of the Metaphysic of Morals (Riga, LV: Johann Friedrich Hartknoch, 1785), pp.1-148.

另一位英國學者John Stuart Mill提出了個人自由可能會受到限制的標準：³⁷

人類之所以有理由與權力可以個別或者集體地對其中任何分子的行動進行干涉，唯一的目的只是為了自我防衛。

That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant.

也就是說，當社會中某位成員的行動已實際造成其它人的傷害，其它人就有理由限制他的行為。

「稜鏡計畫」曝光後的民調顯示，大部分(56%)的美國民眾認同「稜鏡計畫」是可行的方式，且允許政府監控電子郵件和其它網路行為以預防可能的恐怖主義，此民調與2002年的911恐怖攻擊後，美國民眾的立場基本上並沒有改變。³⁸而美國政府也宣稱為了預防下一次911恐怖攻擊事件，「稜鏡計畫」是有其必要性。³⁹

但目的論存在的問題在於解釋因人而異，如何有用、對誰有用，往往因為不同的

觀點與條件，就有不同的結論。也因此，誰能解釋，誰的行為就是符合道德。

從「稜鏡計畫」一事來看，美國政府宣稱是反恐活動的需要，但大多數民眾不是受害者，甚至不是美國民眾，無法體會放棄個人隱私權與達成維護國家安全的重要性。但“稜鏡計畫”，在某種程度擴大了操縱人民賦予政府的權力，讓美國得以維護其國家利益，已是違反國際慣例，等同將觸手伸到其它國家，能為所為而不受約束地監控全球民眾，也掌握國際貿易或是內部重要訊息，鞏固自身國際霸權的優勢。

民主政府為了維護國家安全而需要採取某種程度的秘密行為，違反基本人權，相對於民主、人權、法治的普世價值，顯得格外諷刺。「稜鏡計畫」或許成功預防了可能大規模的恐怖攻擊事件，但人民的基本權利也同樣被侵蝕。因此，如何拿捏國家安全與民主自由，是同等重要的問題。

三、資訊透明化的程度

因此，在網路時代，所有人均透過網路、雲端運算企業上網，但問題在於哪些資料是雲端運算企業可以保留的？將哪些不同

36 Jeremy Bentham, *An Introduction to Principles of Morals and Legislation* (London, UK: T. Payne, 1789), pp.1-378.

37 John Stuart Mill, *On Liberty* (London, UK: John W.Parker & Son, 1859), pp.68.

38 PewResearchCenter, *Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic*, 詳參<http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/>, (2013), 檢索日期：2015年4月12日。

39 Michael Morell, *Michael Morell: Correcting the Record on the NSA Recommendations*, 詳參http://www.washingtonpost.com/opinions/michael-morell-correcting-the-record-on-the-nsa-recommendations/2013/12/27/54846538-6e45-11e3-aecc-85cb037b7236_story.html, (2013), 檢索日期：2015年4月29日。

來源的資料匯集是被允許可以用資料挖掘、大數據等方式進行分析？而何時允許政府看「我的」資料。

威脅個人隱私很多，現在個人資訊的「透明度」將會越來越高，而限制政府過多的要求也許可以構成良好的道德立場。如果社會中的一分子，每個人都清楚任何行為逃不過監視，這將可能成為零犯罪的社會，而且會是很有效率的政府。然而，人們將生活在監控的恐懼之中。安全與效率是政府應當追求的，但最終仍要保留底線，而不能無限制的犧牲一切。

結 論

因此，綜合上述國家、公司、個人的三個角色與探討的關係，本章節將歸納與提出三者角色應有的定位，以讓三者有適當的平衡點，最後從Google商業契約(服務條款)與Edward Snowden事件來看，軍人從網路、雲端運算中學到應有的認知。

一、政府的選擇

如英國史學家John Dalberg-Acton勳爵所言：「權力使人腐壞，絕對的權力使人絕對的腐壞」(Power tends to corrupt and absolute power corrupts absolutely)。縱使國家安全局的網路監控起因於911恐怖攻擊事件，為了給予美國本土更安全的保障。但透過網路監控可以獲得的資訊，難以如黑與白一樣簡單區分出恐怖分子或是善良的美國民眾。

美國一貫採取市場自我管制的保護規律，是源自於傳統上認為對民眾來說不是大政府是好事，也就是管得越少越好，由市場機制自我調節，經濟體系將良好的運作，有限政府會是更好的選擇。根據這概念，市場機制若可以自我調節，政府就應該盡量不要干預，不予以規範。不過，一旦政府試圖以產業自我規範為資訊保護隱私權為主軸，但最終將意識到政府無法卸除保護的責任，也就是多少需要介入市場以保護民眾。⁴⁰

二、公司的立場

雲端運算企業應該自我道德規範，為商業契約(服務條款)提供使用者應有的合理隱私的期待，明確的文字讓使用者清楚瞭解他們的權益。並使用“硬碟是城堡”的概念，確定在雲端運算中的個人所有物將不會未經使用者同意而做其它用途，如廣告或提供非法監控。

三、個人的代價

各國政府以國家安全為由強化對民眾數位生活的監控，我們將無法在網路期待有個人隱私。因此，本研究建議使用者應該採行為保護他們數位資料的安全，至少不要讓想要保護的隱私放在網路上。

不論是對政府或是公司，個人的權益始終處於弱勢，尤其在這個所謂「自由民主」至上的時代，明目張膽的獨裁已經過時的做法。在電影《美國隊長》：酷寒戰士(Captain America: Winter Soldier)裡一句經典

40 Steve Lohr, Online Industry Seizes the Initiative on Privacy, 詳參<http://www.nytimes.com/library/tech/99/10/biztech/articles/11priv.html>, (1999), 檢索日期：2015年4月27日。

名言：「人們需要心甘情願地交出自由」(Humanity needed to surrender its freedom willingly)。⁴¹但現在最流行的獨裁方式，就是讓民眾對民主有一種錯覺，讓民眾認為他們有選擇，但其實沒有。儘管民眾最後瞭解到政府得到的權力已經超過原有的，但民眾選擇不聽或潛意識忽略，這就是政客能夠操弄的關鍵因素。

因此，民眾應當監督政府他們的言行、權力內的行為、責任與相關的社會事務。在民主社會中，需要透過政府政治、監督、討論與反思，直到我們能夠真正擁有自由，在這樣的過程，民眾需要犧牲時間、精力關心重要的社會問題，才能真正使政客不能濫權。

同樣的，公司所提供的服務條款，也是讓使用者以為自己有選擇，但是並不一定。除了品牌名聲大，容易讓人忽略掉隱藏在品牌背後的風險。同儕與朋友之間的使用，互相推薦使用者經驗，也會讓人容易忽略掉其商業契約背後的風險。

然而，透過市場機制是理想的環境，現今娛樂多元與吸引的情況，民眾容易沉溺在安逸的環境，直到發生貼近生活的重大社會事件，才會覺醒意識到需要保障自己。因此，見微知著，透過市場機制抵制不合理契約是有必要的，甚至積極尋求政府立法保障弱勢的大眾人民。

四、保密是軍人的天職

從Google的服務條款與Edward Snowden事件來看，軍人以保密為天職，不但時時需有警覺心。對於網路這種無遠弗屆的影響力，更加需要小心使用。尤其不能將軍方機密在民間網路上傳送與使用，以避免無端被攔截資訊與滲透。而在出營區後的個人行為，也應隨時注意保持軍人的身分，避免在網路上留下個人資訊，甚至與軍方、軍事單位相關的資訊。

參考文獻

1. Albert W. Alschuler, "Interpersonal Privacy and the Fourth Amendment," Northern Illinois University Law Review, Vol.4, (1983), pp.1-58.
2. Jeremy Bentham, An Introduction to Principles of Morals and Legislation (London, UK: T. Payne, 1789), pp.1-378.
3. Thomas K. Clancy, The Fourth Amendment: Its History and Interpretation (Durham, NC: Carolina Academic Press, 2008), pp.1-738.
4. William J. Clinton and Albert Gore, Jr., A Framework for Global Electronic Commerce, 詳參<http://www.w3.org/TR/NOTE-framework-970706>, (1997), 檢索日期：2015年4月10日。
5. John W. Dean, George W. Bush as the New Richard M. Nixon: Both Wiretapped Illegally, and Impeachably; Both Claimed That a

41 Anthony Russo and Joe Russo, Captain America: The Winter Soldier (Burbank, CA: Walt Disney Studios Motion Pictures 2014)

- President May Violate Congress' Laws to Protect National Security, 詳參<http://writ.corporate.findlaw.com/dean/20051230.html>, (2005), 檢索日期：2015年4月29日。
6. Charles Fried, "Privacy," Yale Law Journal, Vol.77, No.3 (1968), pp.475-493.
 7. Lawrence M. Friedman, "The Eye that Never Sleeps: Privacy and Law in the Internet Era," Tulsa Law Review, Vol.40, No.4 (2004), pp.561-578.
 8. Barton Gellman and Laura Poitras, U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program, 詳參http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1, (2013), 檢索日期：2015年4月22日。
 9. Google, Google Terms of Service, 詳參<http://www.google.com/intl/en/policies/terms/>, (2015), 檢索日期：2015年3月22日。
 10. Glenn Greenwald and Ewen MacAskill, NSA Prism Program Taps in to User Data of Apple, Google and Others, 詳參<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>, (2013), 檢索日期：2015年4月22日。
 11. Quentin Hardy, The Lowdown on Google Drive, 詳參http://bits.blogs.nytimes.com/2012/04/24/the-lowdown-on-google-drive/?_r=0, (2012), 檢索日期：2015年4月24日。
 12. Matthew J. Hodge, "The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com," Southern Illinois University Law Journal, Vol.31, (2006), pp.95-122.
 13. Immanuel Kant, Groundwork of the Metaphysic of Morals (Riga, LV: Johann Friedrich Hartknoch, 1785), pp.1-148.
 14. Orin S. Kerr, "The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?," Connecticut Law Review, Vol.33, No.2 (2001), pp.503-533.
 15. Philip Kotler and Kevin Lane Keller, Marketing Management (Upper Saddle River, NJ: Prentice Hall, 2012), pp.482.
 16. Frederic Lardinois, Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL and Apple Deny Participation in NSA PRISM Surveillance Program, 詳參<http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/>, (2013), 檢索日期：2015年4月10日。
 17. Michael Liedtke, Denials in Surveillance Program Require Decoding, 詳參<http://news.yahoo.com/denials-surveillance-program-require-decoding-000528228.html>, (2013), 檢索日期：2015年4月30日。

- 日。
18. Daniel Lin and Michael C. Loui, "Taking the Byte Out of Cookies: Privacy, Consent, and the Web," *Computers and Society*, Vol.98, No.Privacy (1998), pp.39-51.
19. Ching Yi Liu, "Cloud Computing Internet Privacy," *Taiwan Bar Journal*, Vol.14, No.2 (2010), pp.39-52.
20. Steve Lohr, "Online Industry Seizes the Initiative on Privacy," 詳參<http://www.nytimes.com/library/tech/99/10/biztech/articles/11priv.html>, (1999), 檢索日期：2015年4月27日。
21. John Stuart Mill, *On Liberty* (London, UK: John W.Parker & Son, 1859), pp.68.
22. Michael Morell, "Michael Morell: Correcting the Record on the NSA Recommendations," 詳參http://www.washingtonpost.com/opinions/michael-morell-correcting-the-record-on-the-nsa-recommendations/2013/12/27/54846538-6e45-11e3-aecc-85cb037b7236_story.html, (2013), 檢索日期：2015年4月29日。
23. George Orwell, *Nineteen Eighty-Four* (London, UK: Secker and Warburg, 1949), pp.1-267.
24. PewResearchCenter, "Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic," 詳參<http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/>, (2013), 檢索日期：2015年4月12日。
25. Laura Poitras and Glenn Greenwald, "NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video," 詳參<http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>, (2013), 檢索日期：2015年4月12日。
26. Robert C. Post, "Rereading Warren and Brandeis: Privacy, Property and Appropriation," *Western Reserve Law Review*, Vol.41, (1991), pp.647-680.
27. William L. Prosser, "Privacy," *California Law Review*, Vol.48, No.3 (1960), pp.383-423.
28. Joel R. Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?," *Federal Communications Law Journal*, Vol.44, (1992), pp.195-243.
29. Anthony Russo and Joe Russo, *Captain America: The Winter Soldier* (Burbank, CA: Walt Disney Studios Motion Pictures 2014).
30. Paul M. Schwartz, "Internet Privacy and the State," *Connecticut Law Review*, Vol.32, (1999), pp.815-859.
31. Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," *Southern California Law Review*, Vol.75, (2002), pp.1083-1113.
32. Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*,

- Vol.154, No.3 (2006), pp.477-560.
33. Shaun B. Spencer, "Reasonable Expectations and the Erosion of Privacy," San Diego Law Review, Vol.39, No.3 (2002), pp.843.
34. United Nations, The Universal Declaration of Human Rights, 詳參<http://www.un.org/en/documents/udhr/>, (2015), 檢索日期：2015年3月25日。
35. Ming Li Wang, "Information Privacy in a Network Society: Decision Making Amidst Constant Change," National Taiwan University Law Review, Vol.5, No.1 (2010), pp.127-154.
36. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol.4, No.5 (1890), pp.193-220.
37. Alan F. Westin, "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I - The Current Impact of Surveillance on Privacy," Columbia Law Review, Vol.66, No.6 (1966), pp.1003-1050.
38. Yahoo, Shedding Light on the Foreign Intelligence Surveillance Court (FISC): Court Findings from Our 2007-2008 Case, 詳參<http://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence>, (2014), 檢索日期：2015年4月10日。

作者簡介

李安國先生，中原大學資訊工程學系碩士。曾任中原大學企業管理學系助教。現就讀於中原大學企業管理學系博士班二年級，博士候選人。

嚴奇峰先生，政治大學企業管理博士。任職於中原大學企業管理學系教授兼企業社會責任研究中心主任。



日本航空自衛隊T-400教練機

(照片提供：張詠翔)