國立交通大學

科技法律研究所

碩 士 論 文

職場網路隱私權之研究─

以新竹科學園區之公司為例

Information Privacy of Internet Communication in Workplace

of Hsinchu Science Park

研 究 生：楊筑安

指導教授：劉尚志 博士

中華民國九十七年九月

職場網路隱私權之研究─以新竹科學園區之公司為例

Information Privacy of Internet Communication in Workplace of Hsinchu Science Park

研 究 生：楊筑安　　Student：Chu-An Yang

指導教授：劉尚志博士　　Advisor：Dr. Shang-Jyh Liu

國 立 交 通 大 學

科 技 法 律 研 究 所

碩 士 論 文

A Thesis

Submitted to Institute of Technology Law

College of Management

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Technology Law

September 2008

Hsinchu, Taiwan, Republic of China

中華民國九十七年九月

職場網路隱私權之研究—

以新竹科學園區之公司為例

學生：楊筑安　　指導教授：劉尚志博士

國立交通大學科技法律研究所碩士班

摘要

本篇論文的研究重點在於獲得臺灣新竹科學園區科技公司內部的網路監控現況與政策，探討其相關法律爭議，及提出解決的建議。因此除了利用文獻分析法闡述隱私權概論、國內外相關立法介紹及判決評析外，同時利用社會學研究方法中之質性研究，針對數家公司的不同部門、層級的主管與員工進行深度訪談，探求國內科技公司內部進行網路管制與監控的目的、保密規則的內容與公告方式、以及實際進行了哪些網路監控行為。比較員工與主管對於網路監控政策上的認知，以員工而言，多數缺乏認識及警覺；以主管而言，明知細節但基於管理上之理由，不願明白告知。

此訪談結果的差異性更進一步指出目前科技公司採取的方式為目的性宣示政策但是全面監控員工電子郵件與網路使用行為，其已涉及基本權權利衝突的憲法問題，應以比例原則加以檢視此政策之合理性。唯臺灣國內法院判決甚少，且偏向資方，政府應基於勞資雙方地位不平等，介入並制定明確的規範，除了讓公司網路監控政策完全透明化，最重要的是必須提供員工申訴的管道或救濟的途徑，也可將國內文獻少見的實證資料提供給後續相關研究者另一個思考方向。

關鍵字：資訊隱私權、職場、監控、保密規則、權利衝突、隱私的合理期待

Information Privacy of Internet Communication in Workplace of Hsinchu Science Park

Student: Chu-An Yang Advisor: Dr. Shang-Jyh Liu

Institute of Technology Law
National Chiao Tung University

ABSTRACT

The lecture is on purpose of acquiring the reality of internet monitoring policy in workplace of technical industrial companies in Hsinchu science park, discussing related legal issues, and bring up some advices of solution to this issue. Therefore, literature review analysis has been used to expound introduction of privacy, relevant regulation and judgement analysis of overseas and internal. Also, qualitative research is used on depth interview with different departments and positions in various companies to obtain the purpose and actual execution of internet controlling and monitoring, content and announcement of confidential policy. Comparing the acknowledgment of both employee and employer, most employees showed lack of recognization and awareness, as for employer showed tendency of not revealing the whole detail of monitoring policies and execution to employees.

Moreover, the difference points out the intentional declaration of the policy, but the company entirely monitors the behavior of employee's e-mail and internet using. It is related to constitutional issue of conflicts of rights, and its reasonableness should be inspected by the principle of proportionality. However, there are only few judgements in Taiwan courts, and it is favor to the management. The government is responsible to make the explicit regulation to improve this condition and the most importance is to provide employees with complaints and remedies besides the monitoring policy in company will be transparent. Finally, the empirical information might be capable to contribute a different direction for further research.

Keywords: Information Privacy, Workplace, Monitoring, confidential policy, Conflicts of Rights, Reasonable Expectation of Privacy

誌謝

首先，我要感謝我的指導教授劉尚志老師。在進行論文研究與撰寫的這段期間，從未給過我任何壓力，讓我得以擁有絕大的自由發揮空間，將本論文主題進行詳細且具整合性的思考，並給予我寬容的時限，讓我能好好完成這份研究。感謝林三元法官當初提供我相關論文主題的參考資料，以及專題討論報告時所給予我的建議與指導。感謝陳銘雄老師，在已使用了三年的電腦壞掉後，及時地慷慨提供他自己的電腦，讓我能夠順利地完成論文的報告跟撰寫。另外，也要感謝倪貴榮老師、王敏銓老師在論文撰寫期間，對於我任性的打擾以及提問，總是十分具有包容心與耐心並詳細解答我的問題。還有王文杰老師、林志潔老師，謝謝你們常常提供的點心，在我士氣低迷之時，總是能讓我振作起來。最後，十分感謝我的口試委員—王立達老師以及東吳大學法律學系的蔡榮耕老師，同意替我審查論文，並在口試時不吝給予我意見與指導，讓我在論文主題與內容上有更多的資料與更深入、正確、清楚的思考與想法，釐清論文所提出的問題。

我很感謝所辦相處了三年的助理們—蔡姐、素萍、玉佩、思妤、逸雲、又萍、婉禎、欣玲、珮瑜，在這段科法所就讀的期間內，給予我工讀機會，讓我沒有經濟上的壓力，並能順利完成學業，還有許許多多生活上的關懷與做事態度的指導，讓我渡過非常多快樂的時光。

在科法所的三年內，除了課業的學習，還有大大小小的活動參與，特別在擔任班代期間，我更加感謝我的同學的配合與參與，以及在研討會時給予的幫助。能夠碰到這麼多優秀且多元化的同學，無疑是我到目前為止的人生中最受到激勵的時光。

能夠進入科法所就讀，真的是一件非常棒的事情。感謝所上的老師給我這個機會進入科法所，讓我得以學習更多學問，打開自己的視野，並在思考與關懷社會上的問題時，能從更多不同的角度切入，不致偏頗。

最後，感謝我的父母與男朋友在我就讀碩士班的時候，所給予我的支持與照顧，包容與關心，讓我能無後顧之憂地渡過這樣人生的菁華時段，未來的日子我會繼續努力，以不負老師的指導與父母的期望！

謹誌于
交通大學科技法律研究所
九十七年九月

目錄

表目錄

圖目錄

第一章　緒論

第一節　研究動機與目的

自網際網路普及於一般民眾生活以降，資訊傳遞的速度、數量、以及便利性皆一日千里，不僅是一般民眾，業界公司也大量利用網際網路做為傳遞資訊的媒介，以加強公司的運作速度與便利性。然而，網際網路固然提供了一快速便捷的資訊傳遞方式，同時也增加了資訊流向與內容無法如同傳統文件遞送系統般容易監控的風險。對於高科技產業界的科技公司而言，其營業秘密便是公司營利甚至是存續的根本，更是不容外洩。於是大多數的科技公司皆設立有管制資訊流通的規章以防止公司的機密資訊外洩，其中很重要的一環便是網路監控(internet monitoring)。

網路監控是由軟體於非實體的網際網路上對流通的資訊內容進行檢索或是監看，對於監看者不僅有可避免人工作業的便利性，鎖定受監看者身分的特殊性，也同時具有可不被受監看者發現的隱密性，甚至也不會因監看的行為而導致資訊流通速度的延滯[1]。當公司認為員工在網路上所進行的行為不符合其規範時，由於網路監看具有可鎖定受監看者的特殊性，可以很快地鎖定違反規則的員工並進行處分，如民國八十八年世界先進離職工程師竊取機密案[2]、民國九十年聯華電子公司開除員工案[3]、以及民國九十一年臺灣積體電路製造股份有限公司離職經理洩密案[4]，皆是由於以網際網路為媒介進行對外的資訊流通。不論是否為蓄意致使公司

---

[1] David Brin 著，蕭美惠譯，《透明社會─個人隱私 v.s.資訊自由》，頁 87-92，先覺(1999)。

[2] 請參見民國 88 年 4 月 18 日，自由時報，二六版，報導世界先進離職工程師竊取機密資料案。民國 87 年 8 月，一位即將離職的工程師將研發資料交予另一不知情同事，由該員工將資料傳遞至公司外部，該公司因此訂立「資訊系統安全管理規則」，並成立資安小組。隨後該小組藉由網路監控系統查獲一位產品研發工程師於離職前，將研發相關資料利用電子郵件傳送至自己家中的個人電腦。

[3] 請參見錢世傑著，《獵殺隱私時代─10 個讓你失去隱私的理由》，頁 34-35，三民(2004)。民國 90 年聯電董事長透過公司內部網路，向每一位員工發布公開信，談論公司營運狀況，期許員工共體時艱、更加努力。部分員工將此信轉寄予於其他電子公司任職的友人，致使公開信內容於公眾媒體上曝光，並影響聯華電子公司股價。該公司 MIS 部門早已裝置好之網路監控系統，對員工於電腦上的所有行為進行側錄，遂利用該系統資料庫內之記錄鎖定轉寄郵件之員工。該公司遂以「不務正業」等名義，開除十數位員工，並對其餘三百多位員工處以「觀察名單」處分。

[4] 請參見民國 91 年 3 月 7 日，中國時報，一版，報導台積電員工洩密事件。四名台積電 MIS 部門發現員工利用網路郵件將一些 IC 設計資料傳送至公司外部，台積電除處分員工之外，並加強其「機密資訊保護政策(Proprietary Information Protection, PIP)」，並對公司內部資訊建立了分級保密的制度。

遭受損害，只要公司認定其行為損及公司利益，即可懲處員工[5]。自此之後，各公司對資訊方面的管制，除了在政策上對員工嚴加宣導，其對於資訊流通之監控也更形嚴密。

國外各公司監控員工的網路使用情形已經行之有年[6]，除了避免公司機密資訊外洩之外，也同時監控員工是否在上班時間利用公司資源處理私人事務或進行非公事相關的行動[7]。然而這種相當於對員工在電腦上所進行的一切行為進行資料收集的作為，很可能侵犯了員工的隱私權[8]。今若將規模擴大至國家，則即使是在為了國家整體安全的考量之下，仍必須對人民的隱私權加以尊重，而不得加以無限制的監控行為[9]，因此在針對公司監控員工網路使用(例如：電子郵件傳遞、網站瀏覽等等)的議題上，美國在一九九零年代已經獲得政府的重視，並加以修法，擴大監控設備的定義，將電子設備以及無線傳輸也包含在內[10]。以國內而言，雖然在公司內部以保護公司利益為大前提的資訊安全控管部門亦有如同國外公司相同的監控行為，然而卻無相當明確的法規規範此監控行為，更有甚者，在擁有高度科技技術的科技公司，也許員工的網路隱私權已經蕩然無存，此時如有完整法規範的適用，來因應目前科技進步所帶來的隱私危機，但也可以為公司保護營業秘密的手法，找出一個平衡點，這對公司和員工都是必要的。

因此本論文的出發點在於探求國內科技公司實際進行了哪些網路監控行為，員工與主管對於網路監控政策上認知的差異，以及公司公告政策與保密同意的範圍，並希望能利用深度訪談的方式獲得在科技公司的員工針對公司內部網路監控

---

[5] 根據美國管理協會與 ePolicy Institute(www.epolicyinstitute.com) 2007 年發表「2007 Electronic Monitoring & Surveillance Survey」的報告指出，指出超過四分之一的雇主因為員工不當使用電子郵件而開除員工；將近三分之一的雇主則因為員工不當使用網路而開除員工。參見〈The Latest on Workplace Monitoring and Surveillance〉， http://www.amanet.org/movingahead/editorial.cfm?Ed=697

[6] Ellen Alderman, Caroline Kennedy 著，吳懿婷譯，《隱私的權利》，頁 424-438，城邦文化(2001)。

[7] 根據美國管理協會與 ePolicy Institute(www.epolicyinstitute.com) 2007 年發表「2007 Electronic Monitoring & Surveillance Survey」的統計，雇主最在乎員工有任何不當使用網路的情形，因此有百分之六十六選擇監控員工電腦的網路連結，另有百分之六十五使用軟體來設定網站黑名單，意即禁止員工連上不適當的網頁，且這種狀況自 2001 年以來有愈加增加的趨勢。所謂不適當的網頁大致包含以下幾種：成人網站 Adult sites with sexual, romantic, or pornographic content(96%)、遊戲網站 Game sites(61%)、社群網站 Social networking sites(50%)、娛樂網站 Entertainment sites(40%)、購物網站 Shopping or auction sites(27%)、運動網站 Sports sites(21%)、部落格 External blogs (18%)。更有甚者，電腦的鍵盤側錄、使用鍵盤的時間、掃描並檢查電腦的檔案等等的電腦監控比比皆是，亦有雇主利用監視器來監看員工上班時的表現，少數還會使用全球定位系統(GPS)來監控或追蹤手機或員工的門禁卡。參見〈The Latest on Workplace Monitoring and Surveillance〉，http://www.amanet.org/movingahead/editorial.cfm?Ed=697

[8] 請參見前註 6。

[9] 請參見前註 3，頁 119-123。另參見前註 1，頁 419-430。

[10] MICHAEL ROGERS RUBIN, PRIVATE RIGHTS, PUBLIC WRONGS: THE COMPUTER AND PERSONAL PRIVACY 20-25 (1988).

和管制政策，所真正關心的面向是否與法律學者一致[11]，也許可為國內法規範及判決解釋提供另一個思考方向。

第二節　文獻回顧

各文獻對於隱私權的理論與資訊隱私權的發展，以及美國、我國法規範的介紹及判決分析上，均提供本文非常大的幫助。此外，本文所研究者為新竹科學園區公司針對網路隱私權限制應如何回應，因此文獻回顧以本國法之論述為主體。

第一項　期刊論文

科技的快速進步，個人於網路上傳遞的資訊隱私受到重視，與傳統隱私權不同，網路世界取得個人資訊的手法既容易又快速，也因此資訊隱私權漸漸受到學者的注意。由於本文著重在探討網路隱私權，係屬資訊隱私權的內涵之一，在搜尋期刊論文時，分成兩個面向：一為資訊隱私權在國內外的發展，二則是針對企業對員工的網路監控行為之法律爭議與法規範適用之討論。

關於資訊隱私權在國內外的發展，不少學者與實務界人士已有完整的介紹與討論，從隱私權沿革至資訊隱私權之緣由[12]，各國法規及實務見解[13]，以及網路使用與個人資料保護相關法律爭議[14]等，皆有相當詳盡的探討。

公司監看員工網路使用情形的手段，首當其衝的是電子郵件的傳遞[15]。因此大多數的學者主要集中在討論雇主監看員工電子郵件產生的隱私權上的爭議，例如

---

[11] 國內學者多探討公司對於員工電子郵件的監控，甚少對於公司內部網路使用行為作全盤討論，甚至多著墨在憲法權利衝突，公司內員工是否有隱私的合理期待等等理論，缺乏公司內部相關實證資料，特別是在臺灣科技公司內部情形，也許已經比我們所想像的要嚴重多了。請參見本章第二節第一項期刊論文的敘述。

[12] 楊敦和，〈美國法上隱私權之發展〉，《輔仁法學》，第二期(1983)、謝祥揚，〈論「資訊隱私權」〉，《東吳法研論集》，第三卷(2007)、

[13] 許正忠，〈資訊保護法─美國「隱私權法」之研究〉，《軍法專刊》，第三十一卷第七期(1985)、詹文凱，〈美國法上個人資訊隱私權的相關判決〉，《律師雜誌》，第二三三期(1999)。

[14] 劉靜怡，〈資訊時代的法律與科技（四）─電腦網路之使用與個人隱私權之保障〉，《月旦法學雜誌》，第二十四期(1997)、馮震宇、錢世傑，〈論網路電子商務發展與隱私權之保護〉，《萬國法律》，第一零四期，(1999)、周慧蓮，〈資訊隱私保護爭議之國際化〉，《月旦法學雜誌》，第一零四期(2004)。

[15] 王郁琦，《資訊、電信與法律》，頁 73，元照(2004)。

陳仲嶙、賴文智律師的〈職場電子郵件監視的隱私權問題〉[16]、簡榮宗律師發表在《全國律師》的〈監看員工電子郵件產生的隱私權爭議〉[17]、馮震宇教授的〈企業E化的新挑戰─企業權益與員工隱私權保護的兩難與調和〉[18]、范姜真媺教授的〈企業內電子郵件之監看與員工隱私權〉[19]、程法彰律師於《萬國法律》發表的〈在網路世界中美國對資訊隱私的保護及其對營業秘密之影響〉[20]及《法令月刊》第五十六卷第十期〈中美間對於基於雇用關係中之雇員隱私權的探討〉[21]、劉定基律師在《律師雜誌》第三零七期的文章，〈資訊時代的職場隱私權保護—以台北地院九十一年度勞訴字第一三九號判決為中心〉[22]、黃程貫教授在《臺灣本土法學雜誌》第七十三期的〈雇主監看員工電子郵件之合法界限─台北地院九一年勞訴字第一三九號民事判決評釋〉[23]，皆有針對企業監看員工的電子郵件藉以維護企業的營業秘密的法律爭議進行探討，從隱私權的概念、美國法規及實務見解、國內保護隱私權之法律適用問題，以及相關法律爭議之我國現況檢討等。多數學者認為，只要監看符合1.業務上目的；2.使用侵害員工最小的手段；3.監看過程透明化，亦即監看政策與方法皆能明白揭示下，對於企業監看員工電子郵件的行為是持正面態度的[24]。

另外，關於國內實務見解的評析，范姜真媺教授〈企業內電子郵件之監看與員工隱私權〉[25]、吳兆琰研究員〈從國內外實務見解談企業對員工之電子郵件監控〉[26]、劉定基律師〈資訊時代的職場隱私權保護—以台北地院九十一年度勞訴字第一

[16] 陳仲嶙、賴文智，〈職場電子郵件監視的隱私權問題〉，《網路資訊》(2001)。
[17] 簡榮宗，〈監看員工電子郵件產生的隱私權爭議〉，《全國律師》，第六卷第五期(2002)。
[18] 馮震宇，〈企業E化的新挑戰─企業權益與員工隱私權保護的兩難與調和〉，《月旦法學雜誌》，第八十五期(2002)。
[19] 范姜真媺，〈企業內電子郵件之監看與員工隱私權〉，《臺灣本土法學雜誌》，第六十期(2004)。
[20] 程法彰，〈在網路世界中美國對資訊隱私的保護及其對營業秘密之影響〉，《萬國法律》，第一四一期(2005)。
[21] 程法彰，〈中美間對於基於雇用關係中之雇員隱私權的探討〉，《法令月刊》，第五十六卷第十期(2005)。
[22] 劉定基，〈資訊時代的職場隱私權保護—以台北地院九十一年度勞訴字第一三九號判決為中心〉，《律師雜誌》，第三零七期(2005)。
[23] 黃程貫，〈雇主監看員工電子郵件之合法界限─台北地院九一年勞訴字第一三九號民事判決評釋〉，《臺灣本土法學雜誌》，第七十三期(2005)。
[24] 值得一提的是，在討論國內法規範是否可適用在公司監看員工電子郵件的情形時，多數學者會提到民國八十八年通過的「通訊保障及監察法」，可惜的是，多數期刊文章在討論到此法適用問題，還是以公權力作為該法適用對象，對於民眾之通訊監察行為為主題。雖然法務部的研究意見認為此法處罰對象為一般人民，按理應可適用於私人與私人間的通訊監察行為。但此並非本文之研究重點，且限於篇幅關係，在此不予討論。
[25] 請參見前註19。
[26] 吳兆琰，〈從國內外實務見解談企業對員工之電子郵件監控〉，《科技法律透析》，第16卷第10期(2004)。

三九號判決為中心〉[27]、黃程貫教授〈雇主監看員工電子郵件之合法界限─台北地院九一年勞訴字第一三九號民事判決評釋〉[28]這於 2004 年出刊後的四篇文章，均加入了台北地院九一年勞訴字第一三九號判決作為評析的重點。其中，范姜真媺教授在文章中[29]完整介紹日本對監看員工電子郵件的相關論點及司法判決所揭示的判斷基準，黃程貫教授則是提出德國法上的觀察[30]，認為「德國法上關於此一問題的研究，尤其在此等案例中所應進行之利益衡量及衡量過程中應斟酌之原則與標準，似乎值得我國論者與實務界再進一步理解與思考」，而劉定基律師於其文章中的第三部分及註十八[31]，則舉出國際勞工組織對於雇主監控員工的標準以及歐盟「監控工作場所電子通訊」的工作報告。

第二項　碩博士論文

在國內碩博士論文部分，目前並沒有直接與職場網路隱私權相關的博士論文，而相關的碩士論文則集中在 2000 年至 2005 年，寫作的研究生多數來自法律學院，少部分集中在社會科學學院及管理學院。其中僅有三篇論文於題目可推知其為企業監控與員工隱私權之相關研究，但這三篇作者都並非法律學院的學生。有七篇文章主題為網路使用與資訊隱私權相關研究之論文，文中皆有針對企業監看員工網路通訊有一篇幅的討論。

誠如本節前項所述，由於本文重點為探討資訊隱私權內涵之一的網路隱私權，因此在搜尋學位論文時，分成資訊隱私權在國內外的發展及針對企業對員工的網路監控行為之法律爭議與法規範適用之討論。前者國內有不少研究者已有詳盡的探討[32]，在此就不多做說明。

---

[27] 請參見前註 22。
[28] 請參見前註 23。
[29] 請參見前註 19，頁 8-15。
[30] 請參見前註 23，頁 208-211。
[31] 請參見前註 22，頁 55-56。
[32] 藍培青，〈隱私權在美國演進歷程之研究〉，淡江大學美國研究所博士論文(1997)。詹文凱，〈隱私權之研究〉，國立臺灣大學法律學研究所博士論文(1998)。林欣苑，〈網路上隱私權保護途徑之分析〉，東吳大學法律學系研究所碩士論文(2002)。陳信郎，〈資訊隱私權保障與網路犯罪通訊監察法制〉，國立政治大學法律學研究所(2005)。徐新隆，〈數位時代下資訊隱私權問題之研究─以個人資料保護為中心〉，國立台北大學法律學系研究所碩士論文(2005)。楊澤群，〈數位科技下資訊隱私權保護之研究〉，雲林科技大學科技法律研究所碩士論文(2006)等。有趣的是，還有利用哲學角度來探討管理者與被管理者之間的倫理，與資料蒐集探求我國資訊隱私研究現況的論文，雖不在本論文討論範圍，但也提供給相關研究者另一思考方向。王怡靜，〈由亞里斯多德德性倫理學進路看管理者與被管理者之對待倫理－從隱私權與工作權談起〉，國立中央大學

有三篇文章針對企業監控與員工隱私權相關之研究，則是中央大學資訊管理研究所的林俊名〈電子監視系統對員工隱私侵犯與程序公平認知之影響〉[33]、政治大學公共行政研究所的洪敦彥〈工作場所勞動者資訊隱私權之初探性研究〉[34]以及國防資訊研究所的朱俊文〈由隱私權觀點論企業對員工網路行為監視權之探究〉[35]，三篇雖非法律系所的論文，但文章中皆有以法律層面來探討的部分，亦提供了不同於法律學者的觀點。

另外，由法律學及社會科學研究所所提出的論文當中，並無直接以企業監控與員工隱私權為主題來撰寫的，但與此主題有相關性的論文有七篇，可分為兩個研究範圍：其中有五篇在討論網路使用與資訊隱私權之主題下，將企業監看員工電子郵件歸為現今資訊隱私權侵害態樣之一種，有東吳大學法研所的簡榮宗〈網路上資訊隱私權保護問題之研究〉[36]、中正大學犯罪防治所的邱惠雯〈網際網路使用行為之限制─從隱私權保護觀之探討〉[37]、台灣師範大學政治所的王君軒〈資訊社會下資訊隱私權與資訊自決權之研究－以全民指紋建檔為例〉[38]、以及台灣大學國發所的陳煌勛〈網路隱私權保護之研究〉[39]，另外在中國文化大學的陳以儒〈網際網路上隱私權保護之研究〉[40]，他在第五章網際網路通訊內容隱私權之保護中提到，有關電子郵件監看之相關法規。

另一研究範圍則是有關於通訊監察法制之研究，在中原大學財法所的錢世傑〈網路通訊監察法制與相關問題研究〉[41]一文中，提出了美國的法規範及案例分析，並檢討我國企業實務上之運作狀況、相關法令及法律爭議。雲林科技大學科

哲學研究所碩士論文(2003)。涂季旻，〈我國資訊隱私研究現況與趨勢分析〉，屏東科技大學資訊管理研究所碩士論文(2005)。

[33] 林俊名，〈電子監視系統對員工隱私侵犯與程序公平認知之影響〉，國立中央大學資訊管理研究所碩士論文(2002)。

[34] 洪敦彥，〈工作場所勞動者資訊隱私權之初探性研究〉，國立政治大學公共行政研究所碩士論文(2005)。

[35] 朱俊文，〈由隱私權觀點論企業對員工網路行為監視權之探究〉，國防管理學院國防資訊研究所碩士論文(2005)。

[36] 簡榮宗，〈網路上資訊隱私權保護問題之研究〉，東吳大學法律學系研究所碩士論文(2000)。文中第四章第三節。

[37] 邱惠雯，〈網際網路使用行為之限制─從隱私權保護觀之探討〉，國立中正大學犯罪防治研究所碩士論文(2003)。文中第四章第四節。

[38] 王君軒，〈資訊社會下資訊隱私權與資訊自決權之研究－以全民指紋建檔為例〉，國立台灣師範大學政治學研究所碩士論文(2005)。文中第三章第二節。

[39] 陳煌勛，〈網路隱私權保護之研究〉，臺灣大學國家發展研究所碩士論文(2005)。文中第三章。

[40] 陳以儒，〈網際網路上隱私權保護之研究〉，中國文化大學法律學研究碩士論文(2000)。文中第五章第一項。

[41] 錢世傑，〈網路通訊監察法制與相關問題研究〉，中原大學財經法律研究所(2001)。文中第二章第三節、第三章第四節、第四章第四節，均有針對企業主對於員工通訊監察部分進行國內外法規制度與判決實務，以及相關法律爭議之論述。

法所的吳博文〈通訊監察科技法制之研究〉[42]也有這部分法規範之討論。另外，也有論文以職場中之基因隱私權作為研究重點，例如：中正大學法研所的林孟玲〈就業基因歧視防止之研究〉[43]，東海大學法研所的林慧蓉〈論網際網路資訊安全與隱私之保護--以營業秘密之保護為中心〉[44]，則以企業角度來探討如何在網際網路上預防營業秘密之侵害。

第三項　小結

針對職場網路隱私權的部分，學者於期刊中多半對有條件的公司監看政策採取正面態度，碩士論文部分則僅以國內外法規範之整理及法律爭議為主，兩者較不足之處在於，針對此議題之研究方法多為文獻分析與法規範面之比較，在闡述理論、國外法規介紹與國內法律適用及問題爭議的研究已十分詳盡，但卻相當缺乏公司內部的實證資料。因此本論文之研究重點除了文獻分析與比較法外，更加入了質性研究的深度訪談方式，藉此獲得台灣新竹科學園區科技公司內部的監控政策現狀，更重要的是，加入了不同部門、不同層級的主管與員工的意見，可以更清楚知道是否因為制度設計或法規欠缺，造成目前的失當，而政府是否需介入管制或制定法規範才能得到員工隱私權和公司財產權的平衡點，以期在公司對員工網路隱私權之限制的議題上，提出建議並供後續研究參考。

第三節　研究方法

本文以文獻分析、比較研究為論文前半部的主軸，論文後半部則以深度訪談為重點，除了瞭解美國與我國隱私權理論與法規範的演進，最主要的研究目的，是希望藉由深度訪談，探索新竹科學園區科技公司監控員工的現況及手法，於此過程中是否因為制度設計或法規欠缺，造成公司網路管制政策的失當。又政府是否需要介入管制，才能讓員工隱私權和公司財產權有一個平衡點。為達本研究目的，本研究將採用下述方式：

一、文獻分析與比較法：

---

[42] 吳博文，〈通訊監察科技法制之研究〉，雲林科技大學科技法律研究所碩士論文(2006)。文中第四章第六節。

[43] 林孟玲，〈就業基因歧視防止之研究〉，國立中正大學法律學研究所碩士論文(2005)。

[44] 林慧蓉，〈論網際網路資訊安全與隱私之保護--以營業秘密之保護為中心〉，東海大學法律學系研究所碩士論文(1998)。

本研究於隱私權之發展、美國法規範及判決、我國制度及判決中，整理各方觀點並加以分析，進一步指出我國法規及判決解釋不足之處。

二、深度訪談法

本文採用社會科學研究方法其中之一—質性研究(qualitative research)中之深度訪談(in-depth interview)方式作為資料蒐集的一種方法[45]。深度訪談為一種非結構式(unstructured interviews)的訪談，意即研究者事先準備訪談大綱(interview guideline)，但僅有主題(theme)，並非具體且特定的一套問題，也不需以特定用語和次序進行提問。在此架構下，訪談者可在訪談過程中向受訪者自由提出相關問題[46]，其最大特色在於訪談內容彈性大，能充分發揮訪談者與受訪者之積極性[47]。本文訪談對象以受到公司政策規範的員工、負責公司監控事項的資訊部門員工以及有決策力的公司主管為主，了解目前實務上的運作方式及不同部門、層級的員工和主管的看法，討論是否因法規欠缺而造成政策失當，抑或是政府需介入管制或制定法規範來避免權利衝突，以期在公司對員工網路隱私權之限制的議題上，可提出建議並供後續研究參考。

第四節　研究範圍及研究限制

如前所述，本論文之研究重點在於發現公司對員工網路隱私權限制之現況，以及探索目前公司網路管制政策是否失當，政府是否需要介入管制，並希望提供另一個思考方向。然而本研究亦有以下限制：

一、研究目的的限制

本研究主要研究方向為職場中網路隱私權之限制研究，其網路隱私權之內容主要包含網路監控和掃描(Internet monitoring and filtering)、電子郵件監控(E-mail monitoring)、即時訊息監控(instant message monitoring)，意即本文討論範圍為一切在網際網路上進行之活動所受到之限制。其實職場隱私權的課題還包括了藥物檢測(drug testing)、封閉式電路錄影監控(closed-circuit video monitoring)、電話監控

[45] 亦有書中稱為質性田野調查(qualitative research)。參見 Earl Babbie 著，陳文俊譯，《社會科學研究方法》，頁 384-386, 409-413，雙葉書廊(2005)。

[46] Ranjit Kumar 著，胡龍騰、黃瑋瑩、潘中道譯，《研究方法：步驟化學習指南》，頁 130-131，學富文化(2002)。亦有書籍稱為「實地研究訪談」，請參見 W.Lawrence Neuman 著，王佳煌、潘中道、郭俊賢、黃瑋瑩譯，《當代社會研究法—質化與量化途徑》，頁 634，學富文化(2002)。

[47] 石之瑜著，《社會科學方法新論》，頁 157-178，五南圖書(2003)。

(phone monitoring)、位置監控(location monitoring)、個性與心理測驗(personality and psychological testing)、以及鍵盤側錄(keystroke logging)[48]等項目，雖並非本論文之主要研究方向，但仍與職場隱私權息息相關，這些部分也與本論文討論之網路隱私權的部分環環相扣[49]，但礙於篇幅及國內文獻、實證資料不足，僅作相關論述，無法做全盤介紹與呈現。

二、資料蒐集之限制

本研究受限於研究者的經驗及資料取得問題，國外文獻只能就既有部分加以分析整理，國內雖然有許多學者探討公司監控員工電子郵件的相關爭議，然而在司法實務判決資料不足，因此在理論部分也僅以台灣相關法制規範作一觀察與探討。

三、研究方法之限制

本論文研究方法採取質性研究之深度訪談方式，針對新竹科學園區幾家公司的員工及主管進行訪談。然而，這樣的研究模式，需要研究者具備相當程度的訪談經驗和技術性，才能在雙方互動中，得到更多、更深入的資訊。另外，研究者針對研究議題的專業性與中立性、選取樣本的代表性，對於本文研究結果及分析皆具有舉足輕重的影響。而且，質性研究之深度訪談方式不適合大規模母群的統計調查研究[50]，訪談結果的代表性也成為一個考量。不過，筆者仍選擇此研究方法，乃是希望能以實務上的運作現況，進行討論分析，在以此為目的之前提下，透過訪談獲得更多相關資訊，即是對本論文相當重要之處。因此，筆者仍以質性研究之深度訪談方式作為主要的研究方法。

第五節　論文架構

本論文將先針對資訊隱私權之國內外發展作一概述，內容包含隱私權之內容以及資訊隱私權沿革，本文並就「網路隱私權」下一定義，再進一步整理我國在隱私權議題上的發展，從大法官解釋延伸出隱私權在憲法上的地位，以及法規範及判決肯定隱私權存在的演進。接下來參酌美國立法例在公司監控員工網路使用

[48] EPIC 網頁上有關 WORKPLACE PRIVACY 的介紹。請參見第三章第一節。

[49] 譬如：封閉式電路錄影監控(closed-circuit video monitoring)以及電話監控(phone monitoring)也是利用機器來進行，鍵盤側錄(keystroke logging) 則與電腦使用脫不了關係、位置監控(location monitoring)，在公司所使用的門禁卡系統，亦是藉電腦設備來做為員工活動的一個紀錄。

[50] 請參見前註 45，頁 420-423。

的法規制度與判決分析，與我國目前相關法規範作一比較。最後藉由深度訪談的結果探討職場內網路管制政策的缺失與改進之建議。

本文共分為六章，第一章為緒論；第二章概述「資訊隱私權之國內外發展」，首先簡介美國隱私權之發展及內容，接下來，介紹資訊隱私權的概念與內涵，並提出本文中對「網路隱私權」的定義，最後簡介我國在隱私權議題上的發展，係以大法官解釋之憲法基礎為主軸，相關法規範作為補充。

第三章為「網路隱私權在職場上所受到之限制與國內外立法例」，提出職場隱私權的相關課題，並加以限縮在本文主要研究方向：在公司裡一切在網際網路上進行之活動所受到之限制原因與方法。第二節則是以美國對公司監看電子郵件及網路使用的法規範及判決分析為主，第三節則以臺灣目前現有規範是否可對公司監看電子郵件及網路使用的方式有所管制，並以臺北地院九十一年度勞訴字第一三九號進行判決分析，第四節則加入國際勞工組織與歐盟、英國以及德國針對此議題之現況與法規的介紹，最後以美國之法規範對照臺灣之現況，可知臺灣法規範不足之處作為小結。

第四章為實證研究，主要分為兩個問題方向：一是「公司內部針對員工使用網路之監控與管制」，又分成三個小題「網路監控與管制的目的」、「保密規則」、「網路監控和管制的方法」，藉由深度訪談獲得更多公司內部相關監控政策與方式的資訊。二是「員工對於公司網路監控與管制政策之態度」，透過不同部門、層級的員工和主管，可以窺見雙方對於公司內部網路監控和管制政策的態度，採肯定態度所抱持的理由，持反對態度的人的看法，抑或其他相關意見，或是否對這種現況根本沒有任何意識，對於網路隱私權的侵害是否並不在意等的態度，了解公司實際運作上的問題點。

第五章為討論，首先針對第四章的訪談內容作一分析，試著找出不同部門、層級的員工與主管對於公司內部網路監控和管制政策的認知上的差異性，以及探討公司實際運作上出現的問題點，在以第三章之學者論述、臺灣判決評析結果為基礎下，擬提出三大討論方向：「公司內是否有合理的隱私期待」、「公司財產權與個人隱私權之權利衝突」、「公司內針對員工網路隱私權之限制」，後者並分成「保密規則是否可拘束員工隱私權」、「同意是否可完全排除隱私權」這兩點進行檢討，最後加上在科技公司裡員工針對公司內部網路監控和管制政策，所真正關心的面向是否與法律學者一致，將來也許可為臺灣法規範與判決解釋之不足提供一個思考方向，亦可作為臺灣在公司對員工網路隱私權之限制之議題上的建議，並供後續研究參考。第六章為結論與建議。

第二章　資訊隱私權之國內外發展

第一節　隱私權概論

本節簡介了美國隱私權的發展，介紹了 Samuel L. Warren 和 Louis D. Brandeis 所發表的文章，以及 William Prosser 提出的四種隱私權侵害類型，美國法院一開始為否定的態度，後來才漸漸接受隱私權的存在。另外，透過分類，可以將難以定義的隱私權界定出一些範圍，因此區分成四種內容，來涵蓋隱私權之多樣性。

第一項　美國隱私權之發展簡介

將隱私權作為一種法律概念而加以討論的，起源於一八九零年由兩位美國律師 Samuel L. Warren 和 Louis D. Brandeis 在 Harvard Law Review 發表「The Right to Privacy」一文，其中引用了 Thomas M. Cooley 法官在一八八零年發表的「A Treatise on the Law of Torts」書中提到的一項個人權利的內容為「to be let alone」—此將隱私的概念明確型塑成隱私權[51]—文中認為此項權利所保護的是個人的思想與情感，為人格權之一種，並從習慣法中推導出隱私權本應受到保護的概念，並指出其概念下的幾個原則：「

一、隱私權不能禁止涉及公共或一般利益的公開；

二、依據法律有傳播的權利時，隱私權不受保護；

三、口頭散佈在無特別損害時，不構成隱私權之侵害；

四、經由本人散佈或其同意時，即無隱私權之存在；

五、散佈內容屬實或散佈者缺乏惡意(malice)不構成抗辯之理由；

六、隱私權被侵害的救濟，可以損害賠償或禁制令或立法科以刑罰的方式。[52]」

---

[51] 詹文凱，〈隱私權之研究〉，國立臺灣大學法律學研究所博士論文，頁 13-19(1998)。

[52] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-220 (1890).

這篇文章將隱私權定義為生活的權利「right to life 」及個人獨處的權利「right to be let alone」。提出之後，雖未獲得極大的重視，但美國法院漸漸分成兩派，一部分法院認為隱私權(right of privacy)的新概念被接受，是一件很可怕的事，另一部分的法院則樂觀其成，期待這種概念被落實[53]。直到案例慢慢累積，美國法院才漸漸接受習慣法中具有隱私權的存在地位[54]。

到了一九六零年，美國著名之侵權行為研究學者 William Prosser 提出四種獨立且分離的隱私權侵害(invasion of privacy)的侵權類型，這四類區別後來被美國侵權行為法(Second Restatement of Tort)採用，並幾乎被美國所有法院所接受[55]，甚至有些州將此概念直接引用於其州法，也使隱私權的保護獲得美國法上的確立及理論的快速成長：

1. intrusion：係指對他人隱居處進行物理性的干擾。”This type of privacy is invaded by physical intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.”

2. disclosure：將私人事務公開揭露，此點為 Samuel L. Warren 和 Louis D. Brandeis 文章中最關注的一點。”the public disclosure of embarrassing private facts about the plaintiff.”

3. false light：以誤導方式將他人隱私公開。”for defendant to present plaintiff to the public in a false light ”

4. appropriation：未經允許使用個人資料。”involves defendant’s unpermitted use, usually for commercial purposes, of plaintiff’s identity, with damage to plaintiff’s dignitary interests and peace of mind.”[56]

第二項　隱私權之內容

隱私權為一獨處的權利(to be let alone)，其目的在於規避私領域事務之公開，

另參見前揭註。

[53] J. THOMAS MCCARTHY, THE RIGHT OF PUBLICITY AND PRIVACY (2d ed. 2008). 資料來源：WESTLAW<http://international.westlaw.com>

[54] 請參見前註 51，頁 20-25。

[55] 請參見前註 53。

[56] William L. Prosser, *Privacy: A Legal Analysis*, 48 CAL. L. REV. 383, 388-407 (1960). See also *Id*.

是一種消極被動的防禦權利[57]，因為這樣的權利內容牽涉到個人主觀性的認知，在時空的演變下會有不同程度的理解，加上隱私權的概念所包含的並非單一的利益，而是具有多樣性的面向與層次，也因此十分難以定義[58]。不過，隱私權的內容也可以使用法律概念來建構，一般來說，隱私權的內容可分成以下四種範疇[59]：

一、身體的隱私(Bodily privacy)：個人的身體、生活與財產具有不受物理性侵入的權利；

二、通信的隱私(privacy of communication)：此與美國憲法第一修正案所規定的言論及出版自由相關，個體具有與他人自由通信的權利；

三、資訊的隱私(Information privacy)：個人具有其資料的控制與處理的權利；

四、私人領域的隱私(Territorial privacy)：設定界限於會被侵入的明確空間或場所。

本論文在下一節中將探討隱私權的第三種範疇：資訊隱私(Information privacy)的發展與內容。

第二節　資訊隱私權沿革

隨著資訊時代來臨，社會的資訊化程度提高，電腦與網路使用的普及，以及各種因科技快速發展而產生的技術，不斷推陳出新，以保護個人資料為中心之資訊隱私權概念當時發展的背景，正是受到科技躍進的影響。因為網路上資料取得容易、快速、成本低廉，受到他人入侵的風險也相對提高，此時不得不擴大隱私權的保護範圍，而個人資訊的一切內容要如何享有並防止被別人利用，成為近代憲法上的重要課題。因此，本節先介紹資訊隱私權在這種背景之下所應運而生的美國法概念，進而由這種控制自身權利之積極性內涵，提供四種資訊隱私權之面向，最後，以本論文討論之重點界定出網路隱私權之定義。

---

[57] 徐新隆，〈數位時代下資訊隱私權問題之研究─以個人資料保護為中心〉，國立台北大學法律學系研究所碩士論文，頁 16-17(2005)。

[58] Daniel Benoliel, Law, *Geography and Cyberspace: The Case of On-line Territorial Privacy*, 23 CARDOZO ARTS & ENT. L.J. 125, 127 (2005).

[59] *Id* at 127-128.

第一項　資訊隱私權在美國法上的概念

所謂資訊隱私權，依美國法上的概念來說，稱為 The right of Information Privacy，根據前節的分類，係指個人具有其資料的控制與處理的權利(the control and handling of personal data)[60]，有學者認為資訊隱私權乃指「非侷限於不讓他人取得我們的個人資訊，而是應該擴張到我們自己控制個人資訊的使用與流向」[61]，亦有認為[62]其意義在於「再沒有通知當事人並獲得其書面同意之前，資料持有者不可以將當事人為特定目的所提供的資料用在另一個目的上」。由此可知，「資訊隱私權的中心思想乃在於：個人不僅是個人資料產出的最初來源，也是其正確性、完整性的最後查核者，以及該個人資料的使用範圍的參與決定者」[63]，亦即將傳統認為隱私權為『獨處的權利(to be alone)』規避私事公開為目的，消極性不受干擾的內涵，轉變成控制自身資訊之積極性權利，實為現代個人資訊保護制度最重要理論之一。

第二項　資訊隱私權的內涵

從資訊隱私權的這種控制自身資訊之積極性，發展出在網路上的隱私權保護客體約略分為四個面向[64]：

一、個人屬性的隱私權 (Privacy of a Person's Persona)：

直接涉及個人領域的第一層次，而可謂「直接」之個人屬性，為隱私權保護的首要對象。例如：一個人的姓名、身份、肖像、聲音等。

二、個人資料的隱私權 (Privacy of Data about a Person)：

此可謂「間接」之個人屬性，當個人屬性被量化成文字敘述或記錄，若其牽涉之資料的特徵係獨特且個人化(unique and personal)，則此等資料即含有高度之

---

60 *Id.*

61 劉靜怡，〈資訊科技與隱私權焦慮—誰有權塑造我的網路形象〉，《當代雜誌》，第一二四期，頁 80(1997)。

62 王郁琦，〈網路上的隱私權問題〉，《資訊法務透析》，十月號，頁 39(1999)。

63 簡榮宗，〈網路上資訊隱私權保護問題之研究〉，東吳大學法律學系研究所碩士論文，頁 66 (2000)。

64 ONLINE 269-70 (Thomas F. Smedinghoff ed., 1996).

個人特性而往往能辨識該個人之本體，而亦應以隱私權加以保護。例如：個人的消費習慣、健檢資料、醫院病歷、宗教信仰、財務資料、工作經歷、前科等各式紀錄。

三、通訊內容的隱私權 (Privacy of a Person's Communications)：

利用電子通訊媒介(例如：網路)進行溝通時，由於電子訊息具有可輕易複製以及截取不易被發現的特性，容易被他人窺探或截取得知私人資訊，而這些私人資訊若不為電子訊息之型態，原不易被他人取得。故此通訊內容應加以保護，以利個人人格之完整發展。

四、匿名之隱私權 (Anonymity)：

匿名發表在歷史上一直都扮演著重要的角色，這種方式通常可以保障人對於社會制度提出批評的意願。畢竟，在群體生活中，集體之價值觀未必與個人之想法相符，此種落差常易引發個人以匿名方式表達其意見之需求，且對於社會之差異性與對當權者的反動，往往是促使社會進步之原動力，而這種類型的意見發表往往需要匿名，以使發表者能在心理上與實質上獲得安全。此種匿名權利之適度容許，常能鼓勵個人之參與感，並保護其自由之創造力空間；而就群體而言，亦能藉此獲得差異性的言論，甚至促進其他個體的迴響或反思，進而使群體而獲得進步之動力。

第三項　本文對「網路隱私權」的定義

本論文探討網路隱私權在職場上所受到之限制，係以電子郵件及網際網路使用情形為主要討論重點，以資訊隱私權的內涵來看，應為通訊內容的隱私權(Privacy of a Person's Communications)所涵蓋之範圍，意即利用電子通訊媒介進行溝通。不過，除了利用電子郵件傳送私人訊息之外，本論文尚包含了於網際網路上的所作的一切行為及紀錄，此亦應屬間接個人屬性之個人資料的隱私權 (Privacy of Data about a Person)保護的資料。因此，本論文對網路隱私權的定義為：「利用電子通訊媒介進行一切與網路有關之行為，包含電子郵件之傳送及網際網路之使用」。

第三節　隱私權在我國的發展

隱私權範圍十分廣泛，以我國憲法第十二條規定為例，其保障人民有秘密通

訊之自由，隱含人民擁有隱私空間的生活權益，此與隱私權之保護相關。但是，以我國隱私權概念發展的歷史來看，最重要的確立莫過於大法官解釋。即使憲法未明文列舉隱私權為基本權之一種，但透過這些解釋，仍建立了隱私權在憲法上的地位，亦可得知隱私權在我國的理論發展。例如：大法官釋字第二九三號指出一般客戶財產上之秘密及客戶與銀行往來資料不得任意公開；釋字第五零九號認為言論自由仍應兼顧對個人名譽、隱私及公共利益之保護，而受到合理的限制；釋字第五三五號則認為臨檢實施之手段，影響人民行動自由、財產權、隱私權等甚鉅；大法官釋字第五五四號亦以通姦為告訴乃論，目的在使受害配偶得兼顧夫妻情誼及隱私，而釋字第五八五號則明白指出隱私權應受憲法第二十二條的保障。

另外，涉及個人資訊處理的資訊自主權也透過大法官的解釋，更加確認其屬於憲法位階的概念。大法官釋字第五六九號、第五八五號均提及個人取得及自主控制資訊之權利，釋字第五八六號更是認為在涉及憲法所保障之資訊自主權與財產權之限制下，是會違反憲法第二十三條法律保留原則的。近幾年來，因為新興科技的發展，對於個人資料保護的重視，而衍伸出資訊隱私權的概念，大法官釋字第六零三號更以「為保障個人生活私密領域免於他人侵擾及個人資料之自主控制」再次確認了他在憲法上的地位。但是，釋字第六零三號也有提到「憲法對資訊隱私權之保障並非絕對」，國家仍得以法律之明確規定限制之。

第一項　大法官解釋

大法官解釋在我國隱私權的發展上，可約略分成三個面向：隱私權、涉及個人資料的處理與取得的資訊權[65]，進而擴展到資訊隱私權的概念，分述如下[66]：

一、於隱私權方面：

大法官釋字第二九三號解釋文指出：「...銀行法第四十八條第二項規定「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密」，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權」。另外，由大法官陳瑞堂、張承韜、劉鐵錚不同意見書則提出：「我國銀行法第四十八條第二項明定：『銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密』。此項法律所規定保守銀行秘密之隱私權亦為人格權之一種，

[65] 李震山，〈資訊時代下「資訊權」入憲之芻議〉，《律師雜誌》，第三零七期，頁 15-16(2005)。
[66] 資料來源：司法院法學檢索系統<http://nwjirs.judicial.gov.tw/Index.htm>

依民法第十八條第一項規定：「人格權受侵害時，得請求法院除去其侵害。」憲法對此雖無直接保障之規定，但依憲法第二十二條規定：「凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障。」第二十三條復明定「以上各條列舉之自由權利，除為防止妨礙他人自由，避免緊急危難，維持社會秩序或增進公共利益所必要者外，不得以法律限制之」。保護人格權不受侵害，為現代法治國家人民應享之權利，無妨害社會秩序、公共利益之可言，故此項權利自亦為憲法所保障，非有必要情形不得以法律限制之...」。

大法官釋字第五零九號解釋文提到：「...言論自由為人民之基本權利，憲法第十一條有明文保障，國家應給予最大限度之維護，俾其實現自我、溝通意見、追求真理及監督各種政治或社會活動之功能得以發揮。惟為兼顧對個人名譽、隱私及公共利益之保護，法律尚非不得對言論自由依其傳播方式為合理之限制」。

以上大法官釋字係基於公共利益之保護，於解釋文中承認隱私的存在。

大法官釋字第五三五號解釋文則是認為：「...臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，均屬對人或物之查驗、干預，影響人民行動自由、財產權及隱私權等甚鉅，應恪遵法治國家警察執勤之原則。實施臨檢之要件、程序及對違法臨檢行為之救濟，均應有法律之明確規範，方符憲法保障人民自由權利之意旨」。此釋字正式出現「隱私權」三字。

大法官釋字第五五四號理由書提到：「...通姦罪為告訴乃論，使受害配偶得兼顧夫妻情誼及隱私，避免通姦罪之告訴反而造成婚姻、家庭之破裂。...」。

而在大法官釋字第五八五號理由書，大法官正式承認隱私權為憲法第二十二條所保障之權利：「...其中隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障（本院釋字第五零九號、第五三五號解釋參照）...」。

二、於資訊權方面：

大法官釋字第五六九號，林子儀大法官協同意見書註十五有論者主張：「應加強保護被害人在刑事訴訟程序上的地位，亦即藉由建立行為人與被害人之和解制度、健全被害人保護制度、擴張被害人之資訊權、費用補助權、賠償請求權等以加強其程序參與」，此係指自訴人調查證據取得資訊之權利。

大法官釋字第五八五號理由書於論述隱私權時，提及個人資料之自主控制。許玉秀大法官一部協同一部不同意見認為立法院應有立法的資訊權[67]。

大法官釋字第五八六號解釋文[68]部份提到：「...則逾越母法關於「共同取得」之文義可能範圍，增加母法所未規範之申報義務，涉及憲法所保障之資訊自主權與財產權之限制，違反憲法第二十三條之法律保留原則...」。

三、於資訊隱私權方面：

大法官釋字第六零三號解釋文正式承認資訊隱私權為個人自主控制個人資料之權利，其憲法上依據為憲法第二十二條：

「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障 (本院釋字第五八五號解釋參照) 。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第二十三條規定意旨之範圍內，以法律明確規定對之予以適當之限制。」

第二項　相關法律規範

---

[67] 許玉秀大法官一部協同一部不同意見：「為了立法和監督，立法院需要充分的資訊，當立法院和政府之間關係融洽的時候，也就是彼此有互信的時候，可以透過立法委員的質詢權與政府機關的答詢義務，取得行使職權必要的資訊，但當雙方的互信遭到破壞的時候，**立法院必須有獨立取得資訊的方法，才能進行有效的監督，這就是所謂的資訊自主權（Recht der Selbstinformation），也就是不假手於其他國家機關，而取得資訊的權力**，立法調查權就是建立在這種資訊自主權之上。...」

[68] 大法官釋字第五八六號解釋文：「財政部證券管理委員會 (後更名為財政部證券暨期貨管理委員會)，於中華民國八十四年九月五日訂頒之「證券交易法第四十三條之一第一項取得股份申報事項要點」，係屬當時之證券交易主管機關基於職權，為有效執行證券交易法第四十三條之一第一項規定之必要而為之解釋性行政規則，固有其實際需要，惟該要點第三條第二款：「本人及其配偶、未成年子女及二親等以內親屬持有表決權股份合計超過三分之一之公司或擔任過半數董事、監察人或董事長、總經理之公司取得股份者」亦認定為共同取得人之規定及第四條相關部分，則逾越母法關於「共同取得」之文義可能範圍，增加母法所未規範之申報義務，涉及憲法所保障之資訊自主權與財產權之限制，違反憲法第二十三條之法律保留原則，應自本解釋公布之日起，至遲於屆滿一年時，失其效力。」

我國憲法上，雖未將隱私權加以明文規範，但是第十條保障人民的居住自由、第十二條人民保障秘密通訊自由、第十三條保障信仰及思想自由、第十四條保障結社自由、第十五條保障生存權、第二十二條則以概括的方式保障人民其他自由及權利，這些均構成隱私權保障的憲法基礎[69]。

我國就隱私權保護之法律規範，在民法修正前，並未將隱私權視為保護的客體之一，民法在八十八年修正後，認為隱私權乃屬於人格權的保障範圍，因此當隱私權受到侵害時，可依第 18 條第一項規定：「人格權受侵害時，得請求法院除去其侵害；有受侵害之虞時，得請求防止之。」請求。並將「隱私」兩字明確規範在第 195 條第一項規定：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」，即將隱私權列為民法上保護的客體。民事訴訟法及非訟事件法亦設有維護當事人或第三人之隱私或業務秘密之法規[70]。

刑法亦有許多與隱私權保護相關之條文，例如第三百一十五條的妨害書信秘密罪、第三百一十五條之一窺視竊聽竊錄罪、第三百一十六條業務洩密罪等，皆有處罰規定，並增訂第三百一十八條之一(洩漏利用電腦設備等而知悉之秘密罪)以及第三百一十八條之二(利用電腦等妨害秘密罪)。另外，刑事訴訟法亦有針對搜索、扣押之要件、程序加以規範[71]。

其他特別法的法規，如：少年事件處理法第八十三條[72]、性侵害犯罪防治法第九條、第十條[73]、兒童及少年性交易防制條例第九條[74]、兒童及少年福利法第十七

---

[69] 請參見前註 51，頁 269-70(1998)。

[70] 民事訴訟法第一九五條之一、第二百四十四條、第三百四十四條、第四百二十六條。非訟事件法第一百零六條：「法人或夫妻財產制契約登記簿，任何人得向登記處聲請閱覽、抄錄或攝影，或預納費用聲請付與謄本。前項登記簿之附屬文件，利害關係人得敘明理由，聲請閱覽、抄錄或攝影。但有**妨害關係人隱私或其他權益之虞者**，登記處得拒絕或限制其範圍」。

[71] 刑事訴訟法第一百二十二條至第一百五十三條。

[72] 少年事件處理法第八十三條第一項：「**任何人不得於媒體、資訊或以其他公示方式揭示有關少年保護事件或少年刑事案件之記事或照片**，使閱者由該項資料足以知悉其人為該保護事件受調查、審理之少年或該刑事案件之被告」。第八十三條之一：「少年受第二十九條第一項之轉介處分執行完畢二年後，或受保護處分或刑之執行完畢或赦免三年後，或受不付審理或不付保護處分之裁定確定後，視為未曾受各該宣告。少年法院於前項情形應通知保存少年前科紀錄及有關資料之機關，將少年之前科紀錄及有關資料予以塗銷。**前項紀錄及資料非為少年本人之利益或經少年本人同意，少年法院及其他任何機關不得提供**。」。

[73] 性侵害犯罪防治法第九條：「中央主管機關應建立全國性侵害加害人之檔案資料；其**內容，應包含指紋、去氧核醣核酸紀錄。前項檔案資料應予保密，非依法律規定，不得提供**；其管理及使用等事項之辦法，由中央主管機關定之」。第十條：「醫院、診所對於被害人，不得無故拒絕診療及開立驗傷診斷書。醫院、診所對被害人診療時，應有護理人員陪同，並應**保護被害人之隱私**，

條[75]、去氧核醣核酸採樣條例第十七條[76]以及下一章節將提到的通訊保障及監察法、電腦處理個人資料保護法、電信法[77]等，皆是透過法律規範來保障憲法上與隱私相關之權利。

行政法方面，亦有明文規範「隱私」並加以保護者，例如：行政程序法第四十六條第一項：「當事人或利害關係人得向行政機關申請閱覽、抄寫、複印或攝影有關資料或卷宗。但以主張或維護其法律上利益有必要者為限。行政機關對前項之申請，除有下列情形之一者外，不得拒絕：一、行政決定前之擬稿或其他準備作業文件。二、涉及國防、軍事、外交及一般公務機密，依法規規定有保密之必要者。**三、涉及個人隱私、職業秘密、營業秘密，依法規規定有保密之必要者**。四、有侵害第三人權利之虞者。五、有嚴重妨礙有關社會治安、公共安全或其他公共利益之職務正常進行之虞者。」；社會秩序維護法第八十三條：「有左列各款行為之一者，處新台幣六千元以下罰鍰：一、故意窺視他人臥室、浴室、廁所、更衣室，**足以妨害其隱私者**。二、於公共場所或公眾得出入之場所，任意裸體或為放蕩之姿勢，而有妨害善良風俗，不聽勸阻者。三、以猥褻之言語、舉動或其他方法，調戲異性者」。

適用以上法規並加以闡明隱私權的司法實務判決，更是有相當多的參考，因不在本論文討論範圍之內，在此就不詳列[78]。

提供安全及合適之就醫環境。第一項驗傷診斷書之格式，由中央衛生主管機關會商有關機關定之。違反第一項規定者，由衛生主管機關處新臺幣一萬元以上五萬元以下罰鍰」。

[74] 兒童及少年性交易防制條例第九條第二項：「本條例**報告人及告發人之身分資料應予保密**」。

[75] 兒童及少年福利法第十七條：「中央主管機關應自行或委託兒童及少年福利機構設立收養資訊中心，保存出養人、收養人及被收養兒童及少年之身分、健康等相關資訊之檔案。收養資訊中心、所屬人員或其他辦理收出養業務之人員，**對前項資訊，應妥善維護當事人之隱私並負專業上保密之責，未經當事人同意或依法律規定者，不得對外提供**。第一項資訊之範圍、來源、管理及使用辦法，由中央主管機關定之」。第四十條：「安置期間，非為貫徹保護兒童及少年之目的，不得使其接受訪談、偵訊、訊問或身體檢查。**兒童及少年接受訪談、偵訊、訊問或身體檢查，應由社會工作人員陪同，並保護其隱私**」。第四十四條：「依本法保護、安置、訪視、調查、評估、輔導、處遇兒童及少年或其家庭，應建立個案資料，並定期追蹤評估。因職務上所知悉之秘密或隱私及所製作或持有之文書，應予保密，非有正當理由，不得洩漏或公開」。

[76] 去氧核醣核酸採樣條例第十一條：「主管機關對依本條例取得之被告及經司法警察機關移送之犯罪嫌疑人之去氧核醣核酸樣本，應妥為儲存並建立紀錄及資料庫。**前項樣本、紀錄及資料庫，主管機關非依本條例或其他法律規定，不得洩漏或交付他人；保管或持有機關亦同**」。

[77] 請參見本論文第三章第三節之介紹。

[78] 與隱私權相關之民事判決：八十七年台上字二四五九號、九十六年上易字第九四號、九十六年重上字第四一七號、九十六年選上字第六號、九十四年上易字第二四三號、九十四年上易字第二零三號、九十三年上易字第六八七號、八十七年上字第七六號、臺灣台北地方法院九十三年訴字第一六八二號、臺灣台北地方法院九十一年勞訴字第一三九號、臺灣屏東地方法院九十三年簡上字第五六號等。與隱私權相關之刑事判決：九十三年台上字第六六四號(判例)、九十七年台上字

第四節　小結

本章第一節簡介美國在歷史上隱私權的發展及內容，以及資訊隱私權之沿革，從隱私權消極保護個人獨處權利的性質，轉變成控制自身資訊的積極型權利，可知隱私權本身涵蓋的範圍十分龐大，且隨時代進步不停擴展。並就本論文欲討論範圍，將網路隱私權定義為：「利用電子通訊媒介進行一切與網路有關之行為，包含電子郵件之傳送及網際網路之使用」。

第二節則是提到我國隱私權於憲法上的基礎，係由大法官解釋所確立，特別在大法官釋字第六零三號明確提到資訊隱私權之內容為個人自主控制個人資料，但並非絕對的保障，仍得以法律加以限制。而我國並未將「隱私權」明定於憲法之中，但仍有許多隱含隱私之意的條文，法律規範也已將「隱私」列為保護的客體，而闡明隱私權之司法實務判決更是不計其數，顯見我國對隱私權的重視。然而，針對新興的「資訊隱私權」的概念，仍有待下章節進行討論。

第三二二四號、九十六年台上字第五五零八號、九十四年台上字第一三六一號、九十四年台上字第五三六號、九十二年台上字第二五七四號、九十年上更(一)字第五三三號、八十六年上易字第二六一七號、臺灣臺中地方法院九十五年聲判字第三一號、臺灣高雄地方法院九十二年易字第九三六號、臺灣台北地方法院八六年判字第三一三三號等。資料來源：法源法律網 http://www.lawbank.com.tw/index.php

第三章　網路隱私權在職場上所受到之限制與國內外立法例

第一節　職場隱私權之範疇與限制

公司為了確認員工的工作表現及公司資訊流通及營業秘密等的安全[79]，監控員工一舉一動的行為早已經不是新聞，而加速這種現象發生的原因不外乎目前只有極少數相關的法律規範以及監控器材成本的低廉，在後者取得容易且在高科技的加持下，體積可以微小到進行員工渾然不知的監控[80]，導致員工在職場上的隱私權漸漸消失。對於企業內部的員工而言，服膺公司所宣誓的資訊管制政策是一件理所當然之事。然而由於網路監控之特性，員工可能不知道自己被監控的程度，加上工時越來越長[81]，導致員工無可避免地在休息時間利用公司網路處理私事或是與朋友連繫。如果此時公司仍一視同仁的對網路進行監控，員工的私人訊息便有可能為公司所掌握。網際網路監控的方式除了針對在網路上流通的數據流直接加以分析之外，也可能利用軟體直接側錄鍵盤訊號，以達到監控員工在電腦上的每一個動作之目的[82]。

依據 EPIC[83]的分類，職場隱私權的課題可大致分為：藥物檢測(drug testing)、封閉式電路錄影監控(closed-circuit video monitoring)、網路監控和掃描(Internet monitoring and filtering)、電子郵件監控(E-mail monitoring)、即時訊息監控(instant message monitoring)、電話監控(phone monitoring)、位置監控(location monitoring)、個性與心理測驗(personality and psychological testing)、以及鍵盤側錄(keystroke logging)[84]等。由此可知，這些侵害員工隱私的行為多數是針對個人資訊的監控與截取，但即使公司主張內部所有硬體或軟體設備均為其所有，但並不表示員工在職場內沒有隱私權。本論文所探討的是網路隱私權在職場上所受到之限制，因此公司對員工電子郵件與網際網路的監控即為本章節討論的重點，第一部分介紹美

---

79 PAUL M. SCHWARTZ, JOEL R. REIDENBERG, DATA PRIVACY LAW 367-9 (1996).

80 A. Micheal Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1481-2 (2000).

81 根據行政院主計處<http://www.dgbas.gov.tw>公布「96 年 1 月薪資與生產力統計結果」，臺灣勞工月平均工時為 188.3 小時，較上年同月增加 13.9 小時，較上月增加 5.2 小時。

82 錢世傑，〈獵殺隱私時代─10 個讓你失去隱私的理由〉，頁 116-118，三民書局(2004)。

83 EPIC，Electronic Privacy Information Center 的簡稱，網站為< http://epic.org>。根據網站上的介紹，其為一個公眾利益的研究中心，建立於一九九四年，其目的為引導公眾的注意力於公民自由議題、隱私權保護、美國憲法第一修正案以及美國憲法價值。EPIC 公開關於公民自由的有償電子郵件信箱以及線上社論─the EPIC Alert。同時也出版關於隱私權、開放政府、言論自由和其他與公民自由相關的重要議題。

84 EPIC 網頁上有關 WORKPLACE PRIVACY 的介紹<http://epic.org/privacy/workplace/>。

國相關立法及判決，第二部分則是我國法規範之討論與判決評析，第三部分加上國際勞工組織與英國、歐盟之現況，最後加以比較美國與我國之缺失與差異。

第二節　美國對公司監控員工電子郵件及網際網路管制之使用規範

美國對公司監控員工電子郵件及網際網路管制之相關規範，可從三個方面探討：第一、從憲法層面來觀察對於私人公司內的監控是否適用於美國憲法第四修正案，此修正案為限制政府搜索的重要依據；第二，介紹聯邦法、州法及習慣法之相關規定，是否可作為員工主張公司違法監控員工行為之基礎，在有例外規定的情形下，公司似乎多可避免相關規定的適用，而得以進行監控；第三、歷年判決顯示了一個趨勢，法院到目前為止仍沒有一個定見，但是多數認為應先確認工作場合是否可讓員工具有「合理的隱私期待(reasonable expectation of privacy)」的認識，才能確認公司的監控行為是否違法。

第一項　憲法

事實上，針對美國憲法第四修正案[85]是否可適用於私人公司內的電子郵件及網際網路的監控行為，透過美國學者及實務界的見解，可得知：

"The extent of employees' privacy right in the workplace depends on whether they work in the public sector or private sector. Because constitutional rights operate primarily to protect citizens from the government[86] 'state action' is required before a citizen can invoke a constitutional right.[87]"

「員工隱私權在職場上的延伸範圍，端視其工作場所屬於 public 場合或是

[85] 美國憲法第四修正案全文為：" 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."

[86] "Even for government employees, the Fourth Amendment offers only limited protection from workplace searches...**The Forth Amendment is only violated if public employees have a reasonable expectation of privacy.** The standard requires balancing the employer's need for control and supervision of workplace with the privacy interests of its employees." See Sarah DiLuzio, Comment, *Workplace E-mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741, 744 (2000). See also O'Connor v. Ortega, 480 U.S. 709(1987) (finding an government employee's expectation of privacy unreasonable when the government actor is the employee's supervisor).

[87] S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 828 (1998).

private 場合。由於憲法所賦予的權力基本上只保護公民之隱私權不受政府侵犯,『國家行為』之作用成為援引憲法權力的必要條件。」

因此，在多數美國人的工作場所屬於私人公司的情形下，於美國隱私權之發展上扮演重要地位的美國憲法第四修正案[88]，實際上無法適用在私人工作場合對於員工電子郵件及網際網路的監控狀況。

部分州的州法[89]立有保護隱私權的明確規範，並提供公務員(public officer)較美國憲法更多的保護。然而，如同憲法第四修正案的解釋，這些規範僅保護公務員(public officer)，而並未將其保護範圍延伸至私人公司的工作場合。但加州是唯一的例外，其州法將對公務員的保護延伸至私有領域，使私人公司的員工也能受到同樣的保護[90]。由此可知，對於公司監控員工電子郵件及網際網路的監控行為，員工只能透過美國聯邦法、州法，抑或是普通法的規定來解決這方面的法律爭議。

第二項　聯邦法

1986 年的電子通訊隱私權法案(Electronic Communication Privacy Act，簡稱 ECPA)[91]乃基於科技的快速發展，於 1968 年制定的 Title Ⅲ of the Omnibus Crime Control and Safe Street Act of 1968(The Wire Tap Statute)[92]—其目的在於管制美國政府以及州政府必須合法才能竊聽，其竊聽設備包含需透過全部或部分有線或電纜之相關電子設備(wire and oral communication)傳輸、攔截[93]—已不足以應付這些新興科技所帶來的衝擊[94]，因此國會通過此法案，補充 1968 年法規之缺失，將電子

---

[88] "The Fourth Amendment of the United States Constitution protects citizen from unreasonable search and seizures by government officials. Although the Fourth Amendment does not explicitly mention a right to privacy, the Supreme Court has long interpreted it to include protection of such a right." See Sarah DiLuzio, *supra* note 86. See also Ex parte Jackson, 96 U.S. 727 (1877); Boyd v. United States, 277 U.S. 438 (1928).

[89] Kevin P. Kopp, *Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy*, 8 SETON HALL CONST. L.J. 861, 867 n.36 (1998). (citing the constitution of Alaska, California, Florida, Hawaii, Illinois, Louisiana, Montana and Washington).

[90] Sarah DiLuzio, *supra* note 86, at 745. See also Porten v. University of San Fransisco, 134 Cal. Rept. 839, 842(Cal. Ct. App. 1976)(recognizing a state constitutional violation even when there is no state action).

[91] 18 U.S.C. §2510-2522 (1994).亦請參見附錄二，在本節所提到之法條，皆有加底線註記。

[92] 18 U.S.C. §2510-2520.為 1934 年 The Communications Act 的修正,其目的在於管制竊聽,在第 605 節中提到："no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to and person"，主要管制對象為聯邦政府之竊聽行為。Michael Rogers Rubin, Private Rights, Public Wrongs: The Computer and Personal Privacy 20-23 (1988).

[93] *Id*.

[94] 例如：無線電話、手機、廣播或者是利用電腦設備所傳輸的資訊等。

通訊(electronic communication)納入規範。

ECPA 禁止意圖或故意地攔截、進入、揭露、或使用他人的有線、口頭、或電子通訊的行為[95]，其對電子通訊(electronic communication)的定義為：

"Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[96]

「任何全部或部分藉由電纜、無線信號、電磁方式、光電方式傳輸有關於記號、信號、文件、圖形、聲音、數據或是任何其他人類創造物的行為。」

ECPA 保護了個人的通訊自由，避免政府在沒有法院命令及正當法律程序的情況下進行監控，也使得第三人在沒有法律授權下，不可以攔截或傳遞他人之訊息，例如網路提供者(internet service providers)。如果任何人、團體或者是美國政府違反 ECPA 之規定，將被課以民事責任[97]，而被害者也可據以請求損害賠償[98]。雖然此法並未明文規範電子郵件納入電子通訊，但根據立法沿革可以很清楚地知道國會的目的是將其包含在電子通訊(electronic communication)的定義[99]，實務上美國法院則是透過解釋的方式將 ECPA 的規範及於電子郵件[100]，也因此成為了於工作場合中保護員工網路隱私權最主要的法律依據。

然而，ECPA 有三種例外，透過這些例外規定加上法院的擴張解釋，即足以使公司輕易迴避或免除相關規定的適用：

一、系統供應商之例外(The service provider exception)

"…an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary

[95] 18 U.S.C. §2511 (1994). See also Kevin P. Kopp, *supra* note 89, at 868-70, which stating ECPA "prohibits the intentional or willful interception, accession, disclosure, or use of wire, oral, or electronic communication".
[96] 18 U.S.C. §2510(12) (1994).
[97] 18 U.S.C. §2522(c) (1994).
[98] 18 U.S.C. §2520 (1994).
[99] Sarah DiLuzio, *supra* note 86, at 760.
[100] Steve Jackson Games, Inc. v. United States Secret Services, 36 F.3d 457 (5th Cir. 1994); Wesley College v. Pitts, 974 F. Supp. 275 (D. Del. 1997).

incident to the rendition of his service or to the protection of the rights or property of the provider of that service…"[101]

「…服務提供者於必要範圍內，為提供服務或保護其權利或財產所附帶進行的監控」，並非不法之行為。學者們認為這是對公司於隱私權的監控所能從 ECPA 的規定獲得的最大豁免權，其來自於如果員工所使用的電子郵件是由公司所擁有的系統提供的[102]，此條例外規定足以全部排除公司監控員工的電子郵件或網際網路行為的責任。事實上，很少法院對公司電子郵件的監控行為使用這條例外，反而是其他兩個例外的擴張解釋更有可能為公司所利用[103]。

二、通常商業過程之例外(The ordinary course of business use exception)

根據 ECPA 之規定[104]，所謂攔截(intercept)，必須以「電子裝置」為之[105]，但基於通常商業使用之目的，由通訊服務提供者或管理者所提供或購買的電子裝置，均非屬 18 U.S.C. §2510(5)(a)所述之電子裝置。縱使這個例外並未適用於工作場合的電子郵件，但仍可將類推適用在電話通訊(telephone communications)的內容，用以在公司進行例行監控員工電子郵件的行為上[106]。

法院提供兩個判斷標準，適用於電話通訊(telephone communications)之通常商業過程例外[107]：

1. 內容判斷法(The content approach)

准許雇主監控與商業相關的通訊(business-related communications)，但不允許

---

101 18 U.S.C. §2511(2)(a)(i) (1994).

102 "Commentators have predicted that most private employers will be exempt from the ECPA under this exemption if they provide their employees with e-mail service through a company-owned system." See Sarah DiLuzio, *supra* note 86, 746.

103 Corey A. Ciocchetti, *Monitoring Employee E-mail: Efficient Workplaces vs. Employee Private*, 2001 DUKE L. & TECH. REV. 26 (2001). 資料來源：DUKE law & technology REVIEW <http://www.law.duke.edu/journals/dltr/>

104 18 U.S.C. §2510(5)(a) (1994).

105 18 U.S.C. §2510(4) (1994)." "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

106 Sarah DiLuzio, *supra* note 86, at 747.

107 Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (holding that an employer cannot escape liability under the ordinary course of business exception for monitoring an employee's personal telephone call). See also Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994) (holding that paltry evidence of bomb threats would not justify an employer's covert monitoring of employee telephone calls).

監控純屬私人性質的通訊，係以監控通訊的內容是否具有正當的商業利益。

2. 背景判斷法(The context approach)

此判斷方式為雇主監控是否具有合法正當的商業理由及事前通知員工的政策，通常會要求雇主監控需考量其範圍及目的之關聯性。

多數法院應可以上述兩種判斷方法適用於員工電子郵件之通訊，對於雇主財產權和員工隱私權之間也將提供一個基本的標準可遵循。

三、同意之例外(Prior Consent Exception)[108]

當一方已經有事前同意通訊的攔截及侵入之情形時，即不受 ECPA 之規範。在公司監看員工電子郵件的情況下，所謂員工之同意，不論明示或默示同意，都係基於以下兩點事實：第一、雇主建立明確的電子郵件監控政策；第二、雇主必須依據一個事實：「員工都被告知過電子郵件監控政策，而且選擇繼續使用這個電子郵件系統」[109]。這點對雇主十分有利，只要其建立了完整的監控政策並盡到通知全體員工之義務，員工使用電子郵件的行為就已經可以被視為同意公司的監控政策了。

第三項　州法及普通法、NEMA

州法的保護甚少，除了加州的州法將對公務員的隱私權保護延伸至私有領域，使私人公司的員工也能受到同樣的保護[110]。即使雇主的監控行為並未合乎上述的例外原則，或是員工由於上述的例外原則而受到侵害，州法規根本沒有辦法提供協助，畢竟沒有任何一州曾經通過專為員工的電子郵件隱私而制定之法規[111]。

---

[108] "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State."18 U.S.C. §2511(2)(d) (1994).

[109] Sarah DiLuzio, *supra* note 86, at 748.員工繼續使用電子郵件的事實，即便是沒有什麼選擇而需使用公司電子郵件系統，仍係為一種默示的同意。

[110] 但在 Flanagan v. Epson America Inc. (Cal. Super. Ct. Jan. 4, 1991)一案中，加州法院拒絕將加州竊聽法規定的範圍延伸至私人公司員工的電子郵件通訊中，法院指出這種擴張隱私權的概念，應由立法者來作決定，不應由司法者越俎代庖。

[111] Sarah DiLuzio, *supra* note 86, at 749.

當員工認為雇主侵犯他的電子郵件或網路隱私權時，普通法是最有可能對這些缺失進行補救的，最常被引用在員工對於雇主監控其電子郵件所作的主張之侵權行為法的隱私權案件類型[112]為隱居的侵害(unreasonable intrusion into the seclusion of another)[113]。然而員工卻往往必須面對符合所有要件的困難，也就是侵權行為的兩項要件：「侵入性的管理(highly offensive conduct)」及「隱私權期待(expectation of privacy)」。若雇主已向員工表明將監控其電子郵件，員工很難證明雇主的管理方式是侵入性的，再加上雇主付薪水讓員工在公司提供的工作場所工作，並提供所有使用電子郵件的設備，員工也很難證明在工作場所具有合理的隱私權期待，也因此雇主對於普通法的規範並無太大擔憂[114]。

針對以上情形，美國國會提出一個立法上的建議，稱為 The Notice of Electronic Monitoring Act (NEMA)[115]，試圖去規範雇主必須事先知會員工，關於員工會被電子監控的事實。在雇用時，課以雇主告知員工其電子監控政策的義務，並在每年或政策改變之時提醒員工注意。告知員工電子監控政策的內容應包含監控類型、頻率、方式、以及對經由監控所取得的資訊將如何使用，然而，當雇主具有合理的懷疑，認為員工試圖在工作上進行「有害(harmful)」或是「非法(illegal)」行為時，可免除這項義務。若這法規實行，對於員工在工作場合中電子郵件及網路的隱私權保護將會是一個正面的力量，可以迫使雇主必須注重員工在職場上的隱私，並慎選他們用來進行電子監控的方式[116]。可惜礙於公司團體的壓力，此法案目前尚未通過施行。其他具有相關規定之法案，例如：The National Labor Relations Act (NLRA)，亦受到同樣的遭遇。

第四項　判決分析

---

[112] 美國侵權行為法上將侵害的隱私權案件分成四種類型：1. 對他人隱居處進行的無理由的干擾(Unreasonably intrusion into the seclusion of another)；2. 對他人姓名或是肖像權的侵害(Appropriation of the other's name or likeness)；3. 無理由的對他人私生活的公開(Unreasonable publicity given to the other's private life)；4. 無理由的以誤導方式將他人隱私置於公開(Publicity that unreasonably places the other in a false light before the public)。Restatement, Second, of Torts 652A(1977).亦可參見王郁琦，資訊、電信與法律，元照出版公司，2004 年五月，頁 94。

[113] "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be offensive to a reasonable person."「若有人以物理性或是其他任何方式蓄意干涉或侵擾他人的隱居處、或是其隱私或欲隱私之事物，就被認為是侵犯他人隱私。」Restatement, Second, of Torts 652B(1977).

[114] Corey A. Ciocchetti, *supra* note 103.

[115] H.R. 4908, 106 Cong., 2000. 全文請至美國國會圖書館查詢 <http://thomas.loc.gov/cgi-bin/query/z?c106:HR.4908:>

[116] Corey A. Ciocchetti, *supra* note 103.

美國法院針對員工電子郵件的監看有許多判決，其中幾件判決具有指標性的意義，因此學者多半在論述此議題時提出[117]，整理如下：

表 3- 1 美國法院判決整理

案件	案件事實	法院判決
Flanagan v. Epson[118]	以 Flanagan 為首的公司員工提起民事集體訴訟，控告 Epson 公司侵害其隱私權。原告並主張公司在未經員工同意之下監看其電子郵件，違反其對工作場合之隱私期待。	法院認為 1. 即使公司電子郵件設有密碼，但公司身為電子通訊服務提供者，並不違反 ECPA 之規定，因此員工無法期待自己在工作場合中的電子郵件具有隱私的期待。 2. 電子郵件不屬於加州竊聽法賦予私人企業員工的隱私權類型，若要擴張解釋，應透過立法者規範。
Shoars v. Epson[119]	原告發現公司主管會定期閱讀並列印其全部的電子郵件，在向公司反應後，卻遭公司以將電子郵件作為私人用途之理由解雇。原告提出訴訟，認為公司不當解雇並違反加州竊聽法之規定，嚴重侵犯個人隱私權。	法院拒絕擴張解釋加州竊聽法的規範，認為該法僅適用於電話通訊，不包含以文字型態傳送的電子郵件。
Bourke v. Nissan[120]	原告兩人由公司提供之電子郵件的內容包含個人、色情等與商業無關之事，經同事舉發而被公司警告。後向公司表達被監看的不滿後，兩人便被革職。原告向公司提出告訴，認為公司違法監看員工電子郵件已經侵害了憲法上對於隱私權之保障，而且其錯誤解雇違反了公共政策(public policy)。 被告公司則主張原告員工對於其電子郵件並無隱私權的合理期待，且原告有簽署過一份文件，內容關於公司所有之硬體及軟	法院因原告曾簽署過相關文件，認為原告對於其電子郵件並無合理的隱私權期待，而且原告在事情發生之前已注意到公司有監看的行為。 另外，法院也不認為此解雇係違反公序良俗，公司監看行為自也不構成憲法上隱私權保護之違反。

[117] 參見馮震宇，〈企業 E 化的新挑戰—企業權益與員工隱私權保護的兩難與調和〉，《月旦法學雜誌》，第八十五期，頁 100-102(2002)；錢世傑，〈網路通訊監察法制與相關問題研究〉，中原大學財經法律研究所，頁 89-124(2001)等。

[118] Flanagan v. Epson America Inc., No. BC007036 (Cal. Super. Ct. Jan. 4, 1991).

[119] Shoars v. Epson America Inc., No. YC003979 (Cal. Sup. Ct., Los Angeles Cty., 1991).

[120] Bourke v. Nissan Motor Co., No. B068705 (Cal. Sup. Ct., July 26, 1993).

	體，僅限於使用在公司事務上。	
Smyth v. Pillsbury[121]	被告公司提供電子郵件系統供員工使用，並保證不會截錄電子郵件的訊息，或以其內容作為解雇的依據。原告信賴上述原則而與上司通信，卻遭到解雇。解雇理由為於公司電子郵件系統中傳送不適當及不具專業性的內容。原告提出訴訟，指公司之解雇行為違反公共政策(public policy)。	法院認為本案 1. 並無 Brose v. Piece Goods Shop, Inc[122]所揭示之原則：「對於一個合理的人造成實質且高度的隱私權侵害(intrusion is substantial and would be highly offensive to the ordinary reasonable person)」的適用，因為電子郵件之截取並不屬於實質且高度的隱私權侵犯。 2. 原告在傳送不適當言論時，其對隱私權的合理期待已經消失，並自願地使用公司的電子郵件系統，並無任何保護隱私權之實益。 3. 公司在防止不適當言論或非法活動出現於公司的電子郵件系統具有實質的利益，此遠超過對員工隱私權之保護。
Restuccia v. Burk Technology[123]	被告公司的主管可進入公司的電腦系統並監看員工的電子郵件，而且公司電腦系統也會自動將所有電子郵件備分，但是員工完全不知道有此情形。公司主管發現原告兩人互相談論其醜事，便以過度使用公司電子郵件系統加以開除兩人。原告提起公司侵害其隱私權的訴訟。	法院認為 1. 公司政策並未規定員工之電子郵件不可作為私人通信之用。 2. 公司從未明確告訴員工，公司主管可任意監看員工電子郵件的內容或可被儲存。 基於以上兩點，員工得享有工作場合中，電子郵件隱私權之期待。

近幾年，針對公司監看員工電子郵件及網路使用之管制之法律爭議，美國法院判決至今並無明確定見，但顯示了一個趨勢，亦即探討工作場合中是否具有隱私權的合理期待[124]，所謂隱私權的合理期待(reasonable expectation)必須符合兩項要件：第一、員工是否具有真實(actual)且主觀(subjective)的隱私期待(expectation of privacy)；第二、此合理之期待必須符合為社會所認同[125]。從這兩個要件可以衍伸

[121] Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).
[122] Brose v. Piece Goods Shop, Inc., 963 F.2d 611 (3rd Cir. 1992).
[123] Restuccia v. Burk Technology Inc., 5 Mass.L.Rptr.712 (1996).
[124] In re Board of County Com'rs of County of Arapahoe, 95 P.3d 593 (2003); United States v. Simons, 206 F.3d 392 (4th Cir.2000),…etc.
[125] U.S. v. Simons, 29 F.Supp.2d 324 (1998). "...determining constitutionality of search in work place, court must first consider whether employee searched had actual or subjective expectation of privacy, and expectation must have been one that society recognizes as reasonable."

出兩個判斷標準，一在於公司的電腦設備是否為公司所有[126]，另一則是公司是否有明確宣示其監看政策以及員工是否有同意的意思表示(不論明示或默示)[127]。

從歷年法院的見解可得知，員工的電子郵件即便是有個人登入的帳號密碼，只要公司為系統提供者即可合法監看；若公司有完整的電子郵件監看政策並透過員工同意的情形下，員工的電子郵件即不具備任何隱私權的合理期待，由此可推知，針對公司對員工網路使用的監控行為亦可透過前述標準來迴避 ECPA 之規定。

第三節　我國對公司監控員工電子郵件及網際網路管制之使用規範

目前我國法規沒有對於公司監看員工電子郵件或網路管制使用之明確規範，因此僅就具有相關性之法規：民法、刑法以及通訊保障及監察法，在以學者見解為基礎下加以討論。另外，台北地方法院九十一年度勞訴字第一三九號判決也備受學者與實務界人士關注，此節也會詳述其事實與原被告主張，並就法院判決理由加以評析。

第一項　相關法律規範

雖然我國沒有直接予以公司監控員工電子郵件及網路使用規範的法律，但仍有民法、刑法以及通訊保障及監察法之相關法律可供適用，然而，多數條文需透過解釋適用，此還有賴我國法院判決補充。各法規之關係分述如下：

第一款　民法

就隱私權之保護，將隱私權視為人格權的一種[128]，即可依據民法第十八條第一項規定：「人格權受侵害時，得請求法院除去其侵害；有受侵害之虞時，得請求防止之。」也就是，如果認為公司對員工電子郵件的監視構成隱私權的侵害，應可以根據民法第一百八十四條侵權行為之規定請求財產上的損害賠償。

---

126 TBG Ins. Services Corp. v. Superior Court, 96 Cal.App.4th 443 (2002); U.S. v. Angevine, 281 F.3d 1130 (2002); U.S. v. Ziegler, 456 F.3d 1138 (2006); United States v. Angevine, 281 F.3d 1130 (10th Cir.2002),…etc.

127 United States v. Simons, 206 F.3d 392, 398 & n. 8 (4th Cir.2000); Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir.2002); In re Asia Global Crossing, Ltd., 322 B.R. 247 (2005); Thygeson v. U.S. Bancorp (D.Or. Sept. 15, 2004); Thygeson v. U.S. Bancorp (2004) ; State v. Young, 974 So.2d 601 (2008); In re Asia Global Crossing, Ltd., 322 B.R. 247 (2005),…etc.

128 參見本論文第二章第三節之說明。

至於非財產上的損害賠償，也就是精神上損害的慰撫金，則可依民法第一百九十五條第一項規定：「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。」，以公司監看員工電子郵件的行為造成隱私權的侵害，而有精神上的影響，得加以請求損害賠償。

然而民法的侵權行為，必須具有「故意」、「過失」等主觀可責性。由於公司監看員工電子郵件的政策、抑或是其他可能侵害網路隱私權的情形時，公司通常都以監看之資訊為營業秘密、以及事前已跟員工說明，並取得員工同意為理由，主張公司監看電子郵件的行為不是出於故意或過失，或是背於善良風俗的方法侵害員工隱私權，此時應無法成立侵權行為。學說上比較有爭議的部分，是第三人與公司員工進行網路通訊，公司監看時，可否算是侵害到第三人的隱私而構成侵權行為？以學者見解，仍應依照當時情形與通信內容，及當時的公共政策跟社會習慣或是商業上往來習慣判斷[129]。

第二款　刑法

刑法第三百一十五條規定：「無故開拆或隱匿他人之封緘信函、文書或圖畫者，處拘役或三千元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。」首先以此條文之客觀不法構成要件來看，何謂「封緘」？電腦有無加密、防火牆有無使用的區別不無爭議。對此，學者參考德國刑法的規定，認為應解為被侵入的客體如果是電磁紀錄[130]，必須是特別經過加密處理的電磁紀錄[131]。但此一限縮處罰範圍的見解將來是否為實務所採用，似有待觀察[132]。

第二個問題則在於「以開拆以外之方法」，學者提出是否包括「半途攔截封包(package)」的疑問，但基於科技發展的腳步日新月異，有些情形已經不是當時立法者所能預見到的，是否應以擴張解釋之論理，認為開拆以外之方法是否包括半

[129] 簡榮宗，監看員工電子郵件產生的隱私權爭議，全國律師，第 6 卷第 5 期，2002 年 5 月，頁 60-61。

[130] 刑法自九十四年二月修正公布、九十五年七月施行的新條文，已經將電磁紀錄明定於刑法第十條第六項，並在第二百二十二條第二項視為「準文書」。

[131] 惟有學者認為對於經過加密處理的電腦資料不宜解釋成此條文之「他人之封緘文書」，這樣有違刑法罪刑法定主義派生之類推適用禁止原則。林山田，刑法各罪論上冊，2002 年 3 月，頁 247-252。

[132] 請參見前註 129。

途攔截封包，也落在學者的考量範圍之內[133]。

另外，單純只是備份，由程式自行搜尋，並無人為窺視之監看方式，是否就不包含在此條規範內，不無疑問。

刑法第三百一十五條之一規定：「有左列情形之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或者；二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」公司監看員工的電子郵件是否違反此條規定，其第一個關鍵就在於電子郵件之內容或網路使用之行為紀錄是否屬於本條文規定之「非公開之活動、言論、談話」？應視「活動」或「言論」包含的範圍有多大，以言論而言，應不限於口頭上的表達，否則即與「談話」所涵蓋的範圍重覆，通說認為象徵性言論包含思想的表達所呈現的行為，因為電子郵件的內容如果涉及思想的表達應屬於「言論」所保護的範圍，然而網路使用的行為紀錄則很難包含在言論的定義內，其是否為非公開之活動，仍有待釐清。

第二個關鍵則在於公司是否為「無故」？所謂無故，通說解釋為「無正當理由」，且並非以法律有明文者為限。因此公司以保護營業秘密[134]等為理由，監看員工電腦或 E-mail，或者是公司已經公告有此政策抑或獲得員工之同意(簽署保密同意書等)，極有可能被法院視為正當理由，認為員工有此明示或默示的同意，那麼公司的監看並不會違反此條規定[135]。

第三款　通訊保障及監察法[136]

臺灣於八十八年七月實施通訊保障及監察法，該法第三條規定：「本法所稱通訊如下：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。二、郵件及書信。三、言論及談話。前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限」，第二十四條第一項規定：「違法監察他人通訊者，處五年以下有期徒刑」。

員工平日使用公司所提供的電子郵件，是否涵蓋該法所稱的「通訊」，其監視

---

133 請參見前註 129。

134 陳仲嶙、賴文智，職場電子郵件監視的隱私權問題，網路資訊，2001 年 2 月。

135 換句話說，雖然電子郵件的傳輸、文字內容應屬於該條文所謂之「非公開之言論」，公司的監看政策即有可能觸犯刑法，但在「無故」的客觀不法構成要件下，據有正當理由的公司自無觸法的可能。請參見前註 131，頁 247-263。

136 請參見附錄一，本節所提到之條文，皆有加註底線。

行為，算不算是「監察」他人通訊，從第三條第一項來看，也許應該包括在內；但以第三條第二項，如員工使用公司提供之電子郵件並無隱私的合理期待時，是否不適用此法，似有討論之空間。但同法第二十九條第三款另規定，監察他人通訊而「已得通訊之一方事先同意，而非出於不法目的者」時，即不予處罰。因此，公司依本條規定，可透過員工事先簽署同意書(明示的同意)，來避免此法的法律責任，但如果是默示同意，其同意的方式及範圍仍有限制的必要。

惟通訊保障及監察法之立法目的為保障人民秘密通訊自由、確保國家安全、維護社會秩序[137]，以及第二、五、六、七條的條文針對通訊監察行為之限制，過去曾被質疑該法主要只適用於依法行使監察權之公務員，而不及於一般私人或公司[138]。惟法務部八十九年之解釋[139]明確指出第二十四條以下之處罰對象係亦指一般人民。

第四款　其他

有學者提出[140]電腦處理個人資料保護法及電信法亦有可能規範公司的監看行為，前者(簡稱個資法)立法目的為保護個人隱私[141]，於民國八十四年八月公布。從個資法第三條第六款及第七款可看出規範對象為公務機關以及非公務機關。前者指「依法行使公權力之中央或地方機關」，後者則是「前款以外之左列事業、團體或個人：(一) 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。(二) 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。 (三) 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人」，由此可知非公務機關僅有八大行業被列入個資法的規範，非此八大行業之企業僅能以同條第七款(三)來處理。本論文探討之對象以科學園區高科技公司為主，但很明顯地並未列入個資法的規範；即使在非公務機關的八大行業中的公司，若有監看行為，透過個資法第十八條之規定：「非公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得為之：一、經當事人書面同意者。二、與當事人有契約

137 通訊保障及監察法第一條：「為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序，特制定本法。」參見全國法規資料庫<http://law.moj.gov.tw/fn/fn-c.asp>。

138 通訊保障及監察法第二條第二項：「通訊監察，除為確保國家安全、維持社會秩序所必要者外，不得為之。」，同法第五條為對危害國家安全或社會秩序情節重大之通訊監察，第六條為防止他人生命、身體之急迫危險，檢察官口頭通知執行通訊監察，第七條為避免國家安全遭受危害收集情報通訊監察，以就一般公司針對員工進行的電子郵件監看行為，是為了保護營業秘密的目的來看，似無適用之餘地。參見全國法規資料庫 http://law.moj.gov.tw/fn/fn-c.asp。請參見前註 117，頁 96。

139 法務部 89 年 6 月 16 日(89)法字第 000805 號函。

140 請參見前註 117，，頁 95。

141 電腦處理個人資料保護法第一條：「為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」參見全國法規資料庫 http://law.moj.gov.tw/fn/fn-c.asp。

或類似契約之關係而對當事人權益無侵害之虞者。三、已公開之資料且無害於當事人之重大利益者。四、為學術研究而有必要且無害於當事人之重大利益者。五、依本法第三條第七款第二目有關之法規及其他法律有特別規定者。」公司的監看政策在具有特定目的，或經過員工書面同意[142]，抑或是有契約或類似契約之關係[143]，即可規避個資法的規範。綜觀而言，個資法規範對象的限制，針對公司對員工進行電子郵件的監看政策，似無太大的規範作用[144]。

電信法之立法目的則是保障通信安全及維護使用者權益[145]，如果將電子郵件視為電信訊息之一種，此時有人監看電子郵件即為一種個人通訊自由的侵害，應可依電信法第六條的規定加以懲處[146]。然而，電信法之規定應適用在電信事業及專供公私機構、團體或國民所設置，供其本身業務使用之專用電信，對於員工使用公司提供的設備的前提下，是否可因公司監看而適用此法，不無疑問。

第二項　台北地方法院九十一年度勞訴字第一三九號

在利用司法院法學檢索系統 http://nwjirs.judicial.gov.tw/Index.htm 以及法源法律網 http://www.lawbank.com.tw/index.php 進行關鍵字搜尋與「公司雇主是否可以監看員工電子郵件或網際網路使用」的議題相關判決[147]時，很可惜的是，即使到了 2008 年的現在，仍只有一個關鍵性的指引判決[148]，那就是台北地方法院於九十

142 公司會請員工簽署保密同意書，內容多半具有公司監看政策的規範，這屬於員工的明示同意。

143 僱傭契約中之工作規則及保密規則之遵守，應也隱含公司的監看政策規範，透過員工的明示或默示同意，避免違法。

144 請參見前註 117，，頁 95。

145 電信法第一條：「為健全電信發展，增進公共福利，保障通信安全及維護使用者權益，特制定本法；本法未規定者，依其他法律之規定」。

146 電信法第六條：「電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。電信事業應採適當並必要之措施，以保障其處理通信之秘密。」第五十六條之一第一項：「違反第六條第一項規定侵犯他人通信秘密者，處五年以下有期徒刑，得併科新臺幣一百五十萬元以下罰金」。

147 筆者利用的關鍵字為「工作」、「網路」、「隱私」，並未限縮判決時間範圍。

148 為何說是關鍵性的指引判決？事實上，台北地方法院九十一年度勞訴字第一三九號判決在第一章文獻分析中第二節之期刊論文提到，早由 2004 年輔仁大學范姜真媺助理教授於臺灣本土法學雜誌第六十期發表〈企業內電子郵件之監看與員工隱私權〉，及吳兆琰先生於科技法律透析發表〈從國內外實務見解談企業對員工之電子郵件監控〉，以及 2005 年律師雜誌，由劉定基律師發表〈資訊時代的職場隱私權保護—以台北地院九十一年度勞訴字第一三九號判決為中心〉、以及臺灣本土雜誌第七十三期，政治大學黃程貫教授發表〈雇主監看員工電子郵件之合法界限—台北地院九一年勞訴字第一三九號民事判決評釋〉，以上文章在針對雇主監看員工電子郵件的議題上，對此判決均有相當深入的評論。而後再透過檢索系統，已無如此高度相關性的判決出現，因此台北地院九十一年度勞訴字第一三九號可說是唯一、關鍵且具指標性的判決。

二年十二月作成的一項判決─九十一年度勞訴字第一三九號[149]。

第一款　事實

原告七人受雇於被告公司，於九十一年一月十六日接獲集團總經理發送旨為「調薪」之電子郵件，將其轉寄予配偶及摯友，另一原告則是將被告公司九十一年一月十五日向員工公佈屬於重要業務資訊之「人事異動通知」電子郵件轉寄至公司外部自己的帳戶。總經理於同年一月十八日透過電子郵件於公司內部公告：原告將調薪資訊以電子郵件轉寄至公司外部，觸犯公司「工作規則」第十八條第二十二款：「違反勞動契約或本工作規則，情節重大者。」，予以解僱原告。

第二款　原被告主張

原告主張為以下四點，並向被告公司請求薪資、資遣費，並要求被告依侵權行為賠償原告：

第一點、被告公司非法解雇原告。

第二點、被告公司監看員工電子郵件係侵害原告之隱私權，有損害勞工權益之虞。

第三點、被告公司之工作規則並未約定員工不得將公司業務資訊轉寄他人，且公司之秘密是有管制的，原告所寄發的內容是否為公司之機密事項，似有疑義。

其次，保密同意書僅記載「應嚴守保密規定」，該保密同意書旨在限定業務資訊之範圍，並無被告為確保原告遵守保密規定，得監視原告電子郵件之相關文字，原告縱簽署保密同意書，並不當然放棄其受憲法保障之言論自由、秘密通訊自由

[149] 參見司法院法學檢索系統 http://nwjirs.judicial.gov.tw/Index.htm。雖然台北地方法院九十五年度勞訴第九號、九十五年度勞訴字第二十九號所陳述事實似與本論文具有相關性，畢竟公司監看員工電子郵件的最大目的為防止公司資訊外洩，此兩案公司均為原告，係以員工違反勞動契約及營業秘密法之規定洩漏公司機密資料。兩案雖有使用電腦儲存公司資料，但並非以電子郵件為洩漏方式，前者被告在非職務所需時登入公司電腦，以「手抄」方式重製店面資料與客戶資料，後者被告則是以仲介經理人之身分得知之客戶資料及銷售物件資料「口頭」洩漏於另家公司，因此不在本論文討論範圍內。值得一提的是，在九十六年度板小字第五五三四號判決中，被告提出的抗辯理由第四點中，認為事務所並未制定電子郵件使用政策，也未列入勞動契約內，致使其對此產生合理的隱私期待，事務所如此行為侵犯憲法秘密通訊自由及牴觸通訊保障及監察法第 24 條。可惜的是，判決中並未表明原告係利用何種方式得知被告轉寄機密資料至被告個人信箱，僅提到原告「輾轉得知」；再者，法院判決理由也未針對被告所提出「隱私合理期待」之抗辯有任何進一步的探究。

或隱私權。且被告公司監視之範圍應以原告是否將屬於被告公司行動電話業務之資訊以電子郵件方式遞予他人為限，被告公司僅以避免營業秘密外洩為由，未慮及是否有其他有效可行之方法，逕行全面監視原告之電子郵件，該監看手段不具正當性。

再者，被告公司事前未告知原告其有對員工電子郵件進行監視，亦未於發現原告將電子郵件作私人目的使用後對原告作出警告。

第四點、被告公司未事先告知原告本件電子郵件是否屬於密件，如果是密件應依營業秘密法特別標示，否則員工無法分辨。原告七人遭解雇所轉寄電子郵件，係全公司員工均會收到且可互相轉寄之電子郵件，且非屬「薪資保密」之範圍。另一原告僅因工作需要將郵件轉寄至自己之電子郵件信箱，並未洩漏予第三人，自無被告公司所指稱洩密之事實。

被告公司則是主張其經營高科技產業，營業內容涉及高度機密，對於規範員工使用公司電子郵件與員工保密義務之要求嚴格，以免員工因不當使用電子郵件而侵害公司機密而對公司造成損害。原告之行為已經違反被告公司與其簽訂之勞動契約、公司工作規則、保密同意書、及被告公司之「薪資保密」政策、相關之電子郵件使用規範。且為保護營業秘密，對員工使用電子郵件設有監看措施，以防止資訊外洩，原告事實上已充分知悉此監看政策，因此被告公司實無侵害原告言論自由及隱私權。

第三款　判決理由

法院判決理由第一點表明，原告雖轉寄上述「人事調動」及「調薪」之電子郵件，但被告公司並未標示屬於營業、人事、財務或技術秘密事項，致原告疏未注意，就社會價值判斷上，並非不能期待被告先對原告採取解僱以外之適當懲處，且予警告，若原告再有此類行為，再予以解僱。因此認為被告公司解雇原告不符合勞基法之規定，不生解雇效力。

惟法院針對公司監看員工之電子郵件，是否侵害員工之言論自由、秘密通訊自由或隱私權等基本權利，有以下之見解：

第一、應視員工是否能對其在公司中電子郵件通訊之隱私有合理期待，若公司對於員工電子郵件之監看政策有明確宣示，或是員工有簽署同意監看之同意書，則難以推論員工對於自身電子郵件隱私有一合理期待。又若無法有合理期待，則應另視有無法律明文禁止雇主監看員工之電子郵件。

第二、被告公司曾於八十九年十月二十日以電子郵件向被告公司員工公告：不得將公司內部往來文件洩漏、轉寄、寄發、郵寄予非屬員工之第三人，並將隨時監視且於必要時採取懲戒措施。足認被告公司已事先宣示，電子郵件之使用，應以日常公務上之必要為原則，嚴禁以電子郵件對外傳遞有關公司之營運及技術機密，將隨時監視員工電子郵件之傳遞，以免洩密。被告公司既已事先宣示公司對於員工電子郵件之監看政策，自難認為原告對於其自身電子郵件之隱私有合理之期待。

第三、我國並無法律明文禁止雇主監看員工之電子郵件，且原告於八十九年十月二十日收到上述公告監看之電子郵件後，並未表示反對，應認原告已默示同意被告公司提供之電子郵件系統是供業務用途，且使用被告提供之電子郵件帳號已寓含同意被告監視使用用途。則被告為保護公司營業秘密及達成合法商業目的，所為監看行為，並不符合侵權行為中關於侵入之要件，且因原告之同意而阻卻違法。

第四款　判決評析

九十一年度勞訴字第一三九號是我國第一個，也是到目前為止為一一件針對公司監看員工電子郵件議題提出相關見解的判決，然而，對於原告提出的主張，並未就各點提出更完整、深入之討論，也未釐清相關法律適用，實屬可惜：

第一、法院提出應視員工是否能對其在公司中電子郵件通訊之隱私有合理期待的見解，認為若公司已公告監看政策，或者是員工有簽署同意監看之保密同意書，即完全否定員工有隱私的合理期待。惟隱私權所受到憲法上的保障，是否完全受到公司監控行為的限制？當公司也就是雇主的財產權，與員工於工作場合的隱私權相衝突時，應進一步面對使基本權之衝突，以求此兩項權利的調和[150]。台北地方法院認為被告公司已事先公告電子郵件的監看政策，來決定員工在公司應無合理的隱私期待，卻未能深入探究公司監看政策的目的必要性與方法妥當性，監看本質即為員工隱私權之限制，在利益比較衡量下，探討其是否合乎比例原則應為相當重要之前提[151]。當權利衝突時，應如何加以權衡並解決，似應作更完整的討論。不然，直接先否定員工在公司的隱私合理期待，那麼接下來原告提出的

[150] 劉定基，〈資訊時代的職場隱私權保護—以台北地院九十一年度勞訴字第一三九號判決為中心〉，律師雜誌，第三零七期，頁 59-61(2005)。

[151] 范姜真媺，〈企業內電子郵件之監看與員工隱私權〉，臺灣本土法學雜誌，第六十期，頁 18-19(2004)。

其他主張自然也沒有繼續討論下去的必要了[152]。

第二、被告公司以「電子郵件」通告員工公司監看政策的方法，法院認為只要員工未表示反對，即認為員工默示同意公司監看政策。此公司政策之公告方式是否為明確的宣示，又如此片面的通知可否擴張解釋此為勞動契約或工作規則的一部分，進而對員工產生法律上的拘束力，仍有待商榷[153]。

第三、法院僅以員工收到公司監看電子郵件政策的公告，若未表示反對，就認原告已默示同意公司的政策。問題是，員工此時到底同意了什麼？是同意公司的政策還是同意公司的監看行為[154]？員工默示同意的範圍與界線，法院未能詳細說明清楚，僅僅以公司宣示或有簽署保密同意書來決定有無合理的隱私期待。難道所謂的「同意」即代表公司可以進行全面監控，連非業務無關之私人郵件亦可？何況，相關監看措施的內容與範圍的大小，對於員工隱私侵害程度顯然不同。在公司完全沒有揭露任何相關監看措施的範圍與手段的情形下，員工的同意是否得為法律上一有效的同意[155]，進而阻卻違法，法院的解釋應作更嚴謹的檢討。

第四、法院認為公司監看電子郵件的政策，既因員工缺乏合理的隱私期待，公司而得以合法監看，又為何因員工同意公司電子郵件監看政策而阻卻違法？法院在這件事情的判斷上似乎前後矛盾，到底公司監看員工電子郵件的行為是否合法抑或違法，法院沒有前後一致的見解。而且我國雖然沒有明文禁止公司監看員工電子郵件，但是否完全無法透過解釋適用？事實上，雖然台北地方法院否定了原告主張民法上的侵權行為，而且本節第一項所述現行之刑法因罪刑法定主義而無法完全適用外，民法及通訊保障及監察法之相關規定[156]仍然可以作為公司監看電子郵件政策之界限。特別提出的是，通訊保障及監察法第二條第二項：「前項監察，不得逾越所欲達成目的之必要限度，且應以侵害最少之適當方法為之。」在法務部的研究意見[157]下，若認為此法亦可適用於一般人民，則公司監看的範圍在已逾越保護公司營業秘密等目的之必要性，而且監看的手段、方式侵害員工隱私權甚鉅，抑或是公司欠缺明確宣示、員工並未同意的情況下，是否仍應有其類推適用之可能[158]，可惜法院並未加以著墨。

---

[152] 請參見前註 150。
[153] 請參見前註 151。
[154] 黃程貫，〈雇主監看員工電子郵件之合法界限─台北地院九一年勞訴字第一三九號民事判決評釋〉，臺灣本土雜誌，第七十三期，頁 207-208(2005)。
[155] 請參見前註 150。
[156] 通訊保障及監察法第 24、29 條，刑法第 315 條等。
[157] 請參見前註 139。
[158] 吳兆琰，從國內外實務見解談企業對員工之電子郵件監控，科技法律透析，2004 年 10 月，頁

第四節　其他地區或組織對公司監控員工電子郵件及網路管制之現況

除了美國從九零年代開始注意電子通訊的監控外，國際勞工組織早在一九九零年代初期即已著手有關工作場所監控的研究，並於一九九七年依據一九九一及一九九三年的研究報告[159]提出「保護勞工個人資料實施標準(Code of Practice on the Protection of Worker's Personal Data)[160]」—雇主必須符合兩個條件才能對員工進行監控：第一、需告知員工監控的目的與時間；第二、監控方式需特定，並選擇對員工隱私權造成最小的侵害的方式，若雇主要進行秘密且連續性的監控，則應採取更嚴格的實施標準[161]。

英國則是在西元兩千年通過「二零零零年調查權利規制法(RIPA)」，授權政府機關及企業得於特殊情況下監看員工電子郵件通訊及網際網路之使用[162]，與沒有明確規範的美國相同的是對於企業的讓步，並傾向於公司利益的追求。

歐盟最主要保護個人電子通訊的歐盟個人資料處理及電信隱私保護指令(Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunication Sector, Directive 97/66/EC)僅適用於公共系統，並不包含公司內部的私人通訊系統。然而，歐盟對此問題的重視遠超過美國和英國，其看法與美、英兩國相左，偏向保護員工之個人隱私，並承認工作場合中的隱私權亦為一種人權。因此，歐盟於二零零二年五月公佈了一項報告，其內容與工作場合中電子通訊之監控有關[163]，此工作報告提出了雇主若要進行任何監控員工電子通訊的行為，須符合七項原則，監控才能被認為是合法且有正當理由的：

第一、必要性(Necessity)：係指雇主在進行監控行為之前，需基於特定目的且在絕對必要的情況下，採取對個人隱私權侵害最小的方式；

第二、決定性(Finality)：在監控行為下所得到的資訊必須基於特定、明確、合

17-18。

159 請參見前註 84。

160 International Labour Office, Protection of Worker's Personal Data (1997) §6.14. <www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf>

161 請參見前註 150，頁 55-56。

162 請參見前註 117，頁 150。

163 Article 29 - Data Protection Working Party, Working Document on the Surveillance of Electronic Communication in the Workplace, 5401/01/EN/Final WP55, May 29, 2002.此文件係基於 Directive 95/46/EC 之原則所提出的。文件來源：<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf>

法的目的，並符合比例原則；

第三、政策透明化(Transparency)：雇主的政策必須公開、清楚、詳細，員工可隨時查看而且明白知道政策之內容；

第四、合法性(Legitimacy)：雇主的監控需於法有據，且不會侵害到員工的基本權利；

第五、比例性(Proportionality)：監控的個人資料必須適當、有關聯性、而不逾越特定目的；

第六、資料的準確與保留(Accuracy and Retention of Data)：監控所得之相關資料需正確，非必要性的資料則應該刪除；

第七、安全性(Security)：雇主需有適當的設備來確保所獲得之個人資料不會外洩[164]。

德國亦與歐盟的意見相同，實務界採取偏向於個人隱私之保護的見解，並延續套用德國聯邦憲法法院與勞動法院關於電話談話監聽案例所建立的基本原則：「縱使員工所使用者為公務電話，且係進行公務談話，亦得主張『對於本身話語之權利』…每個個人都有權自己決定其話語之聽取對象的範圍…縱使員工事前清楚知悉雇主設有監聽設備，且有進行監聽之可能，被監聽員工亦不至於喪失使一基本權之保障。惟若雇主確實具有重大利益，且基於該利益之保護而具有必要性時，亦供例外地使其監聽行為合法化、正當化」[165]。

第五節　小結

美國在1986年通過的電子通訊隱私法(Electronic Communication Privacy Act of 1986)，其主要目的在於禁止攔截及非法取得未經授權之電子通訊，雖然被拿來作為員工主張雇主違法監控其電子郵件及網際網路使用之法律依據，然而該法本身規定模糊，不是對公司監控員工電子郵件及網路使用情形的直接規範，加上法規本身有許多例外，反而使公司容易迴避相關規定，得以繼續監控員工。歷年法院判決既沒有統一的解釋與判斷標準，但也多未站在員工那一方，同時也顯示一個

[164] *Id* at 13-19.
[165] 請參見前註154，頁210。

趨勢：如果有事先公告監控政策及取得員工同意，員工便缺乏職場中電子郵件及網際網路使用之隱私權應有的合理期待，而缺乏探討公司監控之目的、類型、方式、範圍是否合乎比例原則？而員工又是否在完全瞭解公司監控政策下才同意？

實際上，美國甚至有發行給公司主管的「雇主指導手冊」[166]之參考書，教導雇主應該清楚哪些原則，會有哪些法律爭議，又如何在法律規定的範圍下，正當監控員工的一舉一動，還有分析何種監控設備的使用會侵害隱私權，監控會造成哪些損失之利益衡量等，甚至連同意書之撰寫草稿，都有標準格式可以使用，當然這些格式內並無涵蓋公司的監控手段與範圍，而僅僅是輕描淡寫地寫著「As a employment condition, I understand that the Company may periodically survey, monitor, or review my work performance by using mechanical, electronic, or other methods. To this work performance surveillance, I expressly consent.」[167]，使得員工在範圍不明的狀況之下，輕易地同意放棄自己拒絕被不當監看的權利。在關係員工隱私權與公司財產權的衝突下，美英兩國先選擇了公司的商業利益，自然沒有如同歐盟發布的工作報告內容之細緻的考量，也沒有類似德國對於員工個人資料保護的原則，反而是犧牲了員工的權益。

臺灣的法規並無明確的規範，多數法規僅能透過解釋適用，而且只要在公司有正當理由的監看情況下，此行為既不符合民法「故意」或「過失」的主觀要件，也沒有通訊保障及監察法第二十九條之「非出於不法目的」之情形，因此現況是監看員工的電子郵件其實並不違法。刑法因罪刑法定主義，除非法條有明確指出違法，否則不宜作擴張解釋。與美國 ECPA 的法規相比，臺灣在監控電子通訊的規定過於簡單，而且不夠詳盡，這樣很難對公司監控員工電子郵件及網際網路使用的行為作出有效的管制。雖有賴法院來補充解釋，但實務上只有一個相關判決—九十一年度勞訴字第一三九號，儘管其採取與美國法院相同的見解，以員工在職場中有無合理的期待為依歸，但並未針對監控手段、範圍，同意的內容等進行探討，實屬可惜，這樣似乎無法提供任何建議予立法者參考，也不能補強法規不足之處，自然也就沒有可讓員工有機會申訴的管道了。

166 KURT H. DECKER, A MANAGER'S GUIDE TO EMPLOYEE PRIVACY: LAWS, POLICES, AND PROCEDURES 207-263 (1989). See also KURT H. DECKER, DRAFTING AND REVISING EMPLOYMENT POLICES AND HANDBOOKS 429-447 (2nd ed. 1994).

167 KURT H. DECKER, *supra* note 166, at 447.

第四章　實證研究分析─深度訪談

第一節　研究設計

本文採用社會科學研究方法其中之一─質性研究(qualitative research)中之深度訪談(in-depth interview)方式作為資料蒐集的一種方法[168]。深度訪談為一種非結構式(unstructured interviews)[169]的訪談，其最大特色在於訪談內容彈性大，能充分發揮訪談者與受訪者之積極性[170]。之所以利用質性研究作為研究方法，無不是因為訪談者與受訪者之間的互動，一方面，受訪者可暢所欲言，使其提供更多且深入的陳述；另一方面，訪談者透過受訪者的經驗、對事情的想法和態度，也許可以得到當初蒐集資料時並未預料的情況。本文希望藉由深度訪談的方式，可以得知在科技公司中，進行網路監控的目的與方法，以及保密規則的內容與揭露方式。最後，也會探求不同部門、層級的員工和主管對於網路監控的看法，以期在公司監控員工網路活動的議題上，進行深入討論、提出建議並供後續研究參考。

第一項　訪談人物選擇

作為質性研究的抽樣樣本，其挑選的方式取決與研究主題的關聯性，並非挑選對象的代表性[171]，此為質性研究的特點，稱為非隨意/非機率抽樣(non-probability sampling)[172]。因此，在選擇訪談人物時，係以立意或判斷取樣(purposive or judgemental sampling)[173]作為抽樣的方式。其前提在於研究者在訪談前能夠判斷最

---

168 亦有書中稱為質性田野調查(qualitative research)。請參見 Earl Babbie 著，陳文俊譯，《社會科學研究方法》，頁 384-386, 409-413，雙葉書廊(2005)。

169 研究者事先準備訪談大綱(interview guideline)，但僅有主題(theme)，並非具體且特定的一套問題，也不需以特定用語和次序進行提問。在此架構下，訪談者可在訪談過程中向受訪者自由提出相關問題，請參見 Ranjit Kumar 著，胡龍騰、黃瑋瑩、潘中道譯，《研究方法：步驟化學習指南》，頁 130-131，學富文化(2002)。亦有書籍稱為「實地研究訪談」，請參見 W.Lawrence Neuman 著，王佳煌、潘中道、郭俊賢、黃瑋瑩譯，《當代社會研究法─質化與量化途徑》，頁 634，學富文化(2002)。

170 石之瑜，《社會科學方法新論》，頁 157-178，五南圖書(2003)。

171 請參見 W.Lawrence Neuman，前註 169，頁 346-347。

172 非隨意/非機率抽樣(non-probability sampling)：沒有根據數學機率理論(量化研究所採用的抽樣方法，注重代表性)來挑選母群體中的個體。其目的在於蒐集能夠澄清、深化瞭解的特定個案、事件或行動，尤其是不適用於大規模社會調查的情境下，抽樣就要利用其他的考量來進行。請參見 W.Lawrence Neuman，前註 169，頁 346-347。

173 立意或判斷取樣(purposive or judgemental sampling)：研究者根據對母群、母群構成元素及研究目的的認識，選擇合適的樣本。請參見前註 168，頁 252。研究者可挑選出適用於以下三種情況

佳的資訊來源，以達成研究的目標[174]，此可對受訪者有比較深入的瞭解。筆者選擇新竹科學園區科技公司的主管與員工作為訪談對象，一是科技公司多半具有完整的資訊部門與資安政策[175]，二來則是透過不同層級的訪談，可以試圖了解員工和主管之間對於網路監控政策認知的差異[176]。另外，筆者也特別針對資訊部門的員工進行訪談，希望藉此得知科技公司保密政策的宣示與實際執行網路監控範圍與手法是否有所不同，以及科技公司對於資訊部門本身是否有所管制，此為本次訪談闡述的第一部分。

第二部分則是請主管、員工、資訊部門的員工針對公司網路管制政策提出其看法，歸納整理同意及反對之理由，探求各訪談者是否具有網路隱私權的意識，以及對於網路管制政策真正的關心處。

以下為訪談對象列表，訪談對象分屬五家不同公司：

表 4- 1 訪談人物列表

代號	部門	職稱	訪談日期
A1	通訊	工程師	2007 年 7 月 12 日
A2	IC 設計	工程師	2007 年 7 月 12 日
A3-1	製造	工程師	2007 年 10 月 18 日
A3-2	專利	主管	2007 年 11 月 17 日
A4-1	專利	工程師	2007 年 10 月 23 日
A4-2	設計	主管	2007 年 11 月 24 日
A5-1	製程整合	工程師	2007 年 11 月 10 日
A5-2	資訊	工程師	2007 年 12 月 2 日

由於訪談內容涉及公司保密規則及內部網路監控政策、方法，雖不落入營業秘密法[177]的保護範圍，但仍屬於公司資訊，因此訪談者統一以匿名處理[178]。另外，

的樣本：一、可提供許多資訊的獨特個案；二、難以接觸到、特殊的母體；三、找出特別的個案類型，再作深入研究。請參見 W.Lawrence Neuman，前註 169，頁 349-351。

174 請參見 Ranjit Kumar，前註 169，頁 194-195。

175 網路監控需要技術和成本，因園區的特殊性質與地理位置，園區內的公司多半需要完善的資安政策來保護營業秘密，並具有足夠的經費負擔資訊部門的成本。同時，技術人才的取得也比一般地區要來得容易。

176 科技公司裡的員工，以工程部門為例，依其學經歷背景，可能會比一般民眾對於網路監控更加敏感，可能會對這方面的問題有更多思考與懷疑。另一方面，也跟筆者大學背景有關。

177 營業秘密法第二條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

178 訪談過程部分以電腦繕打紀錄，部分以訪談筆記作為備忘稿。

雖然不同公司有不同的保密政策與監控方法，不過實體作業環境並非考量因素，在此也不詳列公司名稱，並以編號-1，-2 來代表同一家公司的不同部門及層級。

第二項　研究限制

本文研究方法為非結構式之深度訪談，其優點除了彈性大之外，在於研究者可藉此熟悉研究領域中可能相關問題，並蒐集到豐富的資訊。同時，透過與受訪者的互動，可更深入廣泛地交談、討論，了解受訪者更多的想法、對事情的態度與感受[179]。然而，缺點在於對每一個受訪者可能提問的問題範圍不盡相同，導致於遺漏不同受訪者針對同一問題所提供的不同面向、資訊，即使主題類似或緊扣在同一主題上，但因為問題的不固定，訪談者所收集到各受訪者的答案，拿來比較的可能性不大。

另外，深度訪談的訪談者需要更多經驗及技巧，來避免受訪者對於訪談者的不信任，再加上每次訪談都是經驗的累積，從開始時第一位受訪者到結束時最後一位，訪談過程一定會有明顯的差異[180]，這也會影響到受訪者提供的資訊多寡、深度及相互比較性。質性研究之深度訪談比起其他量化方法要有較大的效度(validity)及較低的信度(reliablity)[181]，意即此方法更能捕捉到問題更深層的意義，但也要同時避免因為研究者價值觀的偏見，而降低訪談的品質。

為減少以上缺點所造成研究結果之不客觀性，筆者藉由事先規劃訪談綱要與列出重點問題方向，並於訪談前告知受訪者主題。受訪者也多選擇已在科學園區公司上班的同學及學長姐，降低兩者產生不信任感的因素，在一對一進行下，受訪者也比較會暢所欲言。如此一來，除了受訪者提供的資訊可以更深入問題點外，更可以兼顧相互比較性。

然而，不可避免的是，由於深度訪談不適合大規模母群的統計調查研究[182]，因此在選擇訪談人物時，他們所服務的公司相異造成的實體作業環境不同，雖不在考量範圍裡，但所採樣者也只分屬五家公司，無法通盤代表新竹科學園區每一

---

179 請參見前註 170，頁 170-172。

180 請參見 Ranjit Kumar，前註 169，頁 130-131。

181 效度(validity)和信度(reliablity)涉及測量的品質。前者關注研究者是否正在測量出想要測量的對象或事情，後者則是包含測量變動誤差的程度，也就是可靠性的關注。請參見 Chava Frankfort, David Nachmias 著，潘明宏、陳志瑋譯，《社會科學研究方法》，頁 202-214，韋伯文化(2001)。另請參見前註 168，頁 420-423。

182 請參見前註 168，頁 420-423。

家公司。不過，但受訪者皆隸屬於知名企業，故仍有一定的代表性。

第二節　公司內部針對員工使用網路之監控與管制

訪談第一部分的主題係針對目前公司內部監控員工網路使用之監控與管制的方法為主，並探求公司監控與管制的目的以及保密規則的內容為主。從不同部門、層級的主管或員工可得知對政策內容認知的差異，以及公司頒布的規定與實際執行上是否涵蓋範圍不同。因訪談對象較多，而且針對一些規定、執行方式較為雜亂，因此呈現在內文中非引號內的敘述多半是整理歸納好的資訊。

第一項　網路監控與管制的目的

根據訪談對象 A3-2、A4-2、A5-2 的訪談紀錄[183]，其實對於公司監控員工電子郵件及網際網路使用政策的目的，A3-2 認為在於維護工作績效及工作機密；A4-2 則認為是防止公司 know-how 外洩、防止公司被病毒入侵；A5-2 資訊部門的員工說得更為清楚：「維護公司的資料安全，確保公司的競爭力」。

第二項　保密規則

保密規則，亦有公司稱作資訊安全規則或資安管理辦法(或稱原則、條例)，其規定的重點，A5-2 說「公司是有很多的資訊保安規則還是條例，像是『禁止攜帶 USB』、『禁止攜帶照相式手機』、『禁止利用公司網路進行違反資安原則的行為』。最後一條就包括一些了諸如『禁止上色情網頁』、『禁止傳遞機密資料至外部信箱』…總之，就是『不可將資訊攜出公司』的意思…」。

訪談對象 A 1、A 2、A3-1、A4-1、A5-1[184]雖處於不同公司，但是卻提供了大同小異的公司網路或資訊管理辦法，例如：不可攜帶照相手機、數位相機、攝影機、私人筆記型電腦，電子郵件的附件有大小限制，任何可移除或有傳輸功能的儲存設備，包括隨身碟等皆不可帶入公司，還有一些功能性的網頁的限制，特別是 web-mail(網路免費信箱)、賭博、色情、駭客、圖片或影音等一些不適當的網頁、

[183] A3-2 於 2007 年 11 月 17 日、A4-2 於同年 11 月 24 日、A5-2 於同年 12 月 2 日的訪談紀錄。
[184] A 1、A 2 於 2007 年 7 月 12 日、A3-1 於同年 10 月 18 日、A4-1 於同年 10 月 23 日、A5-1 於同年 11 月 10 日之訪談紀錄。

部落格、MSN 或 Skype 或 BBS 或 FTP，另外，不可上傳或下載或安裝任何程式於電腦上等。

訪談對象 A3-2 算是綜合各家說法：「…方式包括硬體和軟體。硬體部分就是記錄媒體的管制，像是照像機、照相手機、隨身碟、私人筆記型電腦、或是其他的可移除式儲存設備，以及門禁系統的管制。軟體方面包括 internet 的使用要申請、登記、記錄，e-mail 的檔案大小有限制…公司資料也有分成三級[185]…」

最有意思的是，訪談對象 A5-1 告訴筆者，洩漏保密規則的內容也算是違反保密規則。

那麼，大家都是從何處得知保密規則或公司相關禁止規定的呢？多數都會回答在進公司後第一至三個月，公司會有員工訓練，其中一部分上課內容就是在談保密規則，而且會舉一些公司內相關案例，告訴新進員工如果洩漏公司資訊是一個非常嚴重的錯誤，會被解雇等等的內容。另外，針對非新進員工，訪談對象 A4-2 則說「…公司監控員工的方式有公告，而且技術更新是很快的，不可能事事通知，但都會發公告提醒員工注意，不要違反資安規則…而且公告在公司資料庫上可以隨時查詢…」。

第三項　網路監控和管制的方法

訪談對象 A 1、A 2、A3-1、A4-1、A5-1 都提到關於公司管制電子郵件的方式，首先是寄出去的郵件會經過關鍵字搜尋，附件檔案有大小限制(例如：通常限制寄出的檔案大小比外部寄進公司的電子郵件小很多)，以及電子郵件會備份，A 1 甚至提到電子郵件備份的原因：「…因為有商業上的行為，萬一發生什麼事情，才知道責任歸屬…」。

訪談對象 A4-2 則說：「電子郵件的附件、內容，經過關鍵字掃描，如果出現關鍵字或超過大小，會 copy 給老闆，還有連線的網域，也會 copy 一份給老闆。…公司系統會監控，開機登入就開始…」

訪談對象 A3-2 則告訴筆者，每位員工的電腦每天都會由系統備份，紀錄儲存一個月，且全公司的標準都一樣。另外，針對電子郵件及網路使用，Firewall 和 proxy 的設定嚴密，而且利用門禁系統也可以管理員工，有時候會抽檢，不過機會不多。

[185] 訪談對象 A4-2 、A5-2 均有說明公司內部資料根據保密程度分成三至四級。

訪談對象 A5-2 則更為詳細地說明公司內部的管理的方式及手段：

「以我們公司來說，資訊安全部門就是分兩個部門，大致上來說，一個部門負責基礎網路架構，像是包括實體線路配置、機房等一直到另一個部門負責的前部分。但也不是絕對的分界說，像是前段分你管，後段歸我管這樣。舉例來說，本來應該不屬於 A 而是應該歸給 B 管的網頁管制這種東西，反而歸 A 管。A 以及 B 各自有各自權責範圍之內制定的 rule，而所謂的資訊管理規則則看這個部分是屬於 A 還是 B 的部分管理…」

「管理的手段有很多，例如說『e-mail 關鍵字搜尋』、『USB 偵測器』或是『網頁關鍵字監控』等。其中像是網頁關鍵字監控，其實這一招真的很厲害，當你輸入一個網址的時候，其實是送一個 request 到公司的 server，server 會先去把那個網頁 download 下來，然後程式會自動搜索網頁裡的關鍵字，確定合規定才再傳到你的電腦。例如說『game』或是『遊戲』、『download』或是『下載』、『hacker』或是『駭客』這種字是絕對禁止的，要是『色情』、『十八』這種字出現太多也會被擋住，然後程式會自動把這個網頁加入黑名單。當然也可以把一些網頁手動加入黑名單或是從裡面拿掉。其實這樣不只可以防止員工去上一些公司認為『不適當』的網頁，也可以知道那時候是那一個員工想去上這個網頁，因為是由你的電腦提出傳送網頁給公司的 server，這樣就會留下記錄。例如說，當員工去上諸如 104 的人才招募網頁時，系統就會偵測到這網頁上的一些關鍵字，加以記錄，然後老闆就很可能會知道這員工可能想要離職這樣。…限制向外部信箱寄 e-mail，即使經過申請許可的，也會在系統裡保存一份備份，順便副本給老闆一份，內部寄內部也是一樣…而且很可能有人一封封看內容，確認你是不是在傳送公司資訊，我有同事被警告過一次，可是他傳給我的內容，其實跟公司機密無關，只不過是一個操作介面而已…從外部寄進來的信一般而言不擋，但也是會先經過 server 用關鍵字搜索，然後才轉到員工信箱。但是如檔案太大，或是有附加檔案，一般都會直接擋掉，也不會進入 server，以免有病毒或是惡意程式之類的。…」

訪談對象 A5-1 提供：「有一天我的同事加班到很晚，突然發現自己電腦的滑鼠會自己移動，還打開每個資料夾，我才知道原來自己的電腦還可以被遠端操控，而且還不是經過我同意的操作；還有一次，只是想說看看公司內部網頁的每一項裡面是什麼，順手打開公司內部職缺網頁，瀏覽沒多久，老闆竟然跑來問我『你是不是想換部門呀？』，我真的被嚇了一跳，為什麼老闆會知道？…」

第三節　員工對於公司網路監控與管制政策之態度

訪談的第二部分則是以員工或者主管對於公司網路監控與管制政策的態度為中心，請訪談對象就此事發表看法。當然，針對此政策所表達的意見沒有絕對贊成或反對，只是在訪談一般基層工程師時，多數沒有什麼意見，似乎也不在乎公司監控其電子郵件及網路使用的情形，抱著「反正這也不是什麼機密」、「給他看也無所謂」等的態度的員工不在少數，因此，這部分的訪談意見，僅列出部分被訪談者所提供的意見。

第一項　同意理由

訪談對象 A4-2 說：「…當然，公司應盡保密的義務呀，營業秘密法裡面不是有規定…不過工作這麼累，我通常是針對私事執行上較為彈性，但是針對公事就會比較嚴格…而且公司政策一向透明化，什麼都可以查詢…」

訪談對象 A3-2 則認為：「…規範雖然嚴格，但是執行面有漏洞、過鬆…」

訪談對象 A3-1 告訴筆者設備都是公司財產權的一部分，這樣的管理應該算是合理的方式。

第二項　反對理由

訪談對象 A5-1 認為：

「…其實真的不是很有道理。例如說『禁止上不適當的網頁』這一條，就很有問題。當然公司可以說『萬一怎樣怎樣公司的利益會遭到很大的危害』，但是這樣有時候真的是很麻煩。舉例來說，因為我們工時真的都很長，然後也沒有加班費，因為是責任制，所以很晚下班的時候用公司的電腦想要處理一些私人的事情，總不能說私人的事情請回家處理吧！我也算是把私人的時間拿來在公司做公司的事啊！結果，想說要訂火車票，跳一個『互動式網頁違反公司資安規定』的訊息，想上 yahoo 去私人信箱收個信，也一樣，更扯的是第二天副理就來跟我說要注意公司的資安規定，這樣不是很可怕嗎？…相當於我在電腦上做什麼，有人一清二楚，用程式擋網頁，好吧！小心為上我接受，但是這樣就會被記錄下來通知老闆，那是不是我上銀行網頁用信用卡繳電話費，公司也有可能紀錄到我的密碼？也沒

看公司有公布說他們是用什麼方式來管網路的，這樣真的很危險…公司不信任員工，同樣的員工也沒有理由必須百分之百信任公司，不會把蒐集到的資料做什麼用途。更何況，不只是外部網頁，連內部寄 mail 副理那裡也會收到副本…」

訪談對象 A5-2 資訊部門的員工則說：

「.....資訊安全部門只對員工揭露資訊安全管理規則的目的，例如『不可將資訊攜出公司』，而不揭露如何執行這條規則的手段，例如『在公司門口進行臨檢或是實際上到底是用什麼方法對員工在網路上傳遞的資訊進行監控』，但是公司會盡一切手段防止『資訊被帶出公司』這件事情發生.....基本上公司不只不揭露手段，甚至連明確的界線往往也沒有宣告，使得界線對於員工來說往往十分模糊。舉個例子來說，就拿速限當作一個比喻，公司就好像在路邊立個牌子說『禁止超速』，但並不明確的說速限到底是多少，也不說公司是怎麼會知道員工有沒有超速。而當員工超速的時候，公司的基本態度就是暗示你『大家都知道禁止超速，你本來就應該要儘量避免超速，而不是去看犯規的界線在那裡』。所以員工只好律己從嚴，以免違反公司的規定。至於公司到底是用什麼手段逮到你違規，或是這樣的規定到底合不合理，其實大家也都不是很了解，公司也不認為有必要讓員工知道。但是以一個資訊 security 管理者的觀點來說，應該是要這樣做才能好好管理，以免說知道是怎麼管的，就會有人想辦法鑽漏洞。」

第三項　其他訪談內容

有訪談對象針對公司的資訊部門提供了另一個看法：「…既然網路的監控是資安部門，管理網路的也是人，他就有可能取得他所監看的任何資訊，不是嗎？這樣資安部門本身不就是資訊安全管制上最危險的地方？一個什麼機密都看得到的地方，反而最有可能成為洩密的地方吧！就算被監看到的不是什麼很重要的資訊，也是有一種被強制看光光的感覺…」

「…管這麼多，也不知道合不合理，像我們跟另一個部門也不知道是怎麼分的，他們能用的網路資源硬是比我們多，明明他們能接觸到的資料比較機密吧…還有，我常常花時間在等待網路資訊的核可，工作進度趕得要命，要過的關卡卻一大堆，搞得這麼複雜，拖累大家的時間到底為什麼…」

第四節　小結

根據上述訪談紀錄，可以從第一部分及第二部分的內容進行整理歸納。首先就第一部分的內容，整理如下：

一、公司進行網路監控及管制的目的，不外乎確保公司競爭力(員工的工作績效)、維護公司工作資料的安全(防止公司被病毒入侵)以及避免公司機密外洩。

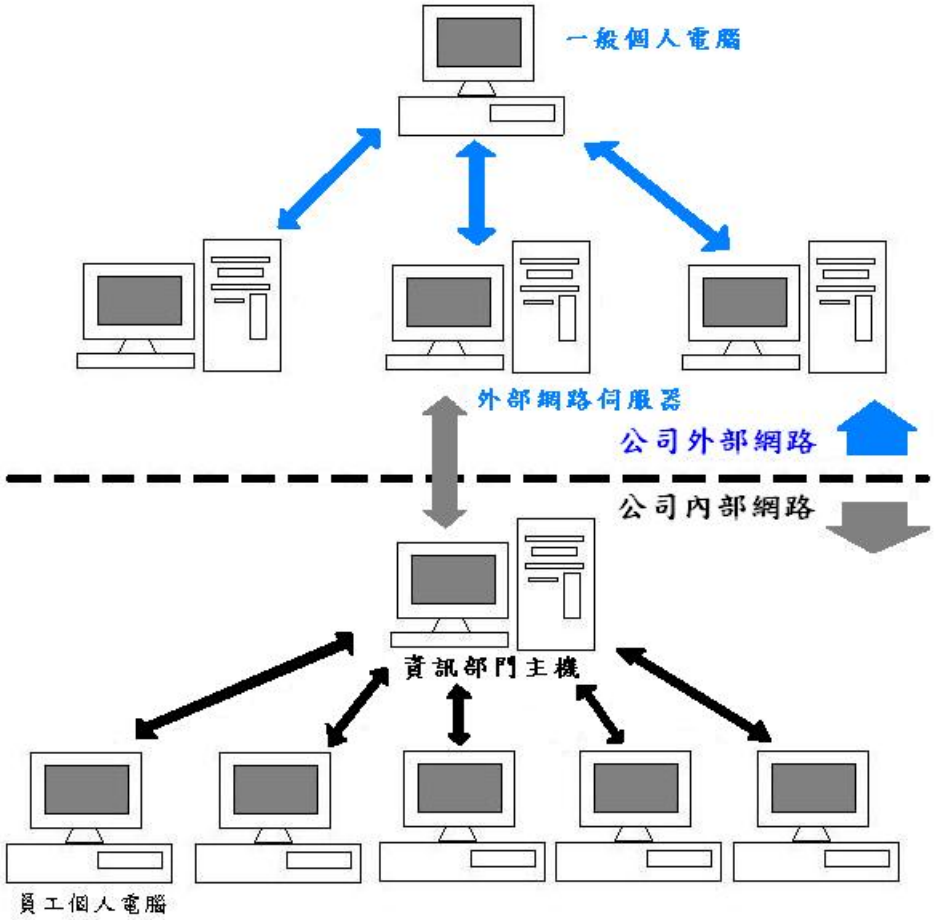
二、保密規則的重點就是不可將資料攜出公司，不論是硬體上或網路上的動作，因此禁止員工攜帶任何可傳輸、儲存的可移除式設備，不可進行可使用網路將公司資訊洩漏的行為，譬如說：禁止連上有功能性的網頁，不可上傳及下載檔案，以及電子郵件傳送附件大小的限制。

三、身為基層工程師的訪談對象 A 1、A 2、A3-1、A4-1、A5-1 都有提到電子郵件的關鍵字掃描、備份及網頁黑名單。身為主管的 A3-2、A4-2 則提供公司的系統只要一開機登入就會開始進行監控，而且也會進行電腦備份，針對電子郵件則是只要超過附件大小限制及搜尋出關鍵字的內容，都會給老闆一份副本，甚至瀏覽的網域也會副本給老闆。

四、身為資訊部門的員工 A5-2 則對公司內部網路的管理方式及手段有更詳細的說明：

(一)公司內部網路的架構，係與外部網路隔離，每一個傳送的電子訊息，包括電子郵件、網頁瀏覽等，都會經過公司資訊部門的主機，才會向外或向內傳送至其他員工電腦，與一般個人電腦直接連向外面網路伺服器不同，亦即所有電子訊息的進出或傳遞，皆由公司內部資訊部門的主機所控制與紀錄，請參見下圖 4-1：

圖 4-1　公司內、外部網路架構



而公司內部網路則將是資訊部門分成兩個組別來管理不同的階段，保密規則即由這兩個組別就自己負責的部分提出規定員工應遵守的內容。

(二)關於電子郵件的處理方式，訪談對象 A5-2 的公司則是遵循三點原則：1.內部郵件往外寄：幾乎絕對禁止，除了被特別許可的一些部門外，抑或是經由檔案大小限制，關鍵字搜尋掃描後，才有機會寄到外部信箱；2.外部郵件寄進公司：會先經過公司資訊部門的伺服器，通過執行檔、病毒掃描、關鍵字、檔案大小限制、和人工篩選的過程後，才能寄進公司；3.以上兩種情形如違反保密規則的規定，例如內容有關鍵字、檔案大小超出限制，以及內部寄內部的郵件，都會給老闆一份副本。以上三種情形，系統都會自動備份。

(三)網頁的瀏覽情形都會被紀錄，老闆也有機會知道，有的公司的員工甚至在被警告後抑或是不小心看到時，才知道公司進行了這樣的監控手段，例如隨時遠端遙控員工的電腦。

第二部分的訪談意見，歸納成三段：

一、同意公司這樣的政策，不外乎是公司為了保障自己的財產權及盡營業秘密法規範之合理保護義務。

二、持反對意見的訪談對象，則認為公司例行性的宣示十分模糊，手段、方法不明，甚至有可能紀錄一些員工的個人資訊，員工不明白有哪些手段，也不知道合不合理。以下圖 4-2 來表示目前管理手段與保密規則的宣示範圍：

圖 4-2　公司內部管理手段與保密規則宣示的範圍示意圖

三、資安部門的權限與設定標準沒有人清楚，有員工認為這樣的過度管制，反而拖累工作效率。

第五章　研究結果分析與討論

第一節　研究發現

根據訪談結果，可以歸納出以下幾項事實：

一、被訪談的基層工程師多數都有意識到公司的監控行為，但是並不在意電子郵件及網路使用的情形是否為公司所監控，亦不明白公司主管針對此事的權限，資訊部門的員工對公司監控的手段與範圍的認知，早已超越基層工程師可得知的內容，甚至可能有專人注意每一封電子郵件的內容抑或是隨時遠端遙控公司任何員工的電腦，觀看員工使用網路之情形。

二、事實上，訪談的多數公司都是在員工開機或登入公司網路系統時，即進行監控，二十四小時的監控過程中不問是否牽涉公司機密及資料，不區分業務上及非業務上的資訊，隨時可掃描、紀錄、備份所有電子郵件的往來內容及網路使用的資料。

三、保密規則僅作目的性地宣示，缺乏明確性的說明，其籠統概括了所有的監控行為，模糊的規定卻採用最高標準的監控，這是公司為了防止一切將資料帶出公司的可能，也符合營業秘密法第二條之規定：「所有人已採取合理之保密措施者」所作出的監控行為，甚至有被訪談者認為公司規定雖嚴格但執行面過於鬆散，無法達到保護工作機密的目的。

四、公司利用內部上課、網頁公告或電子郵件來告知員工有哪些監控政策，但有時技術更新快，無法事事以電子郵件通知，因此員工最常獲取公司監控政策的方式，係藉由公告或是公司資料庫。但此仍係勞動契約或工作規則中之一部分，員工無法表示反對的意見也似乎沒有什麼選擇，抑或是同意卻不知道自己到底同意了什麼內容。

五、多數公司資訊部門屬於一級單位，身為公司監控的中心也是最有能力不被監控的部門，似乎沒有更高層的組織或部門或法規來規範其組成與權限，也因此沒有確立的標準來管理公司的資訊流通。而且公司管制電子郵件與網路使用的目的，不外乎是為了保護公司的營業秘密與確保員工的工作績效，但是透過內部層層關卡來確保公司資料不會外洩的方式，反而可能造成工作效率的低落。

第二節　研究討論

根據研究結果，針對公司監控員工電子郵件及網路使用情形的行為與政策，可以從幾個方面來討論：

一、不論美國還是我國法院判決，都提到一個概念：「合理的隱私期待」，到底員工能不能在公司具有合理的隱私期待，事關重大，判斷工作場合中是否具有「合理的隱私期待」，成為了員工在職場有無隱私權的重要關鍵。

二、公司之所以監控員工，不外乎是為了保障公司財產權，除了營業秘密，還包含了公司擁有內部一切設備的所有權，其與員工網路隱私權的保障，係為一大衝突。

三、公司內對於網路隱私權之限制的具體政策：1.保密規則及相關政策的有無；2.員工的同意與否。前者係屬勞動契約或工作規則之一部分，但是否足以產生拘束員工網路隱私權的效力，而其公告方式、內容，員工是否完全理解，不無疑問；後者則以員工不論明示或默示的同意，依法院認定可作為員工即無在職場擁有合理隱私期待的依據，但是現行公司實際運作狀況是全面進行監控，部份開放權限讓員工知道，或用暗示的方法提醒員工(例如曾經被警告過)，這樣的同意是否有效，似有待商榷。

四、資訊部門身兼行政(管理公司的網路系統)、立法(保密規則及公告的頒布)、司法(利用監控找出違規的員工，交由主管懲處)的功能，這種球員兼裁判的地位，公正性自然受到質疑。以下即從這三點進行討論。

第一項　公司內是否有合理的隱私期待

公司內是否具有合理的隱私期待，依美國及我國法院的見解，為審酌這類案件時最先考慮之關鍵：第一、公司身為設備提供者(電腦、網路等)，多數人均認為在上班時本不應利用網路進行私人事情之處理，因此與員工有無設定電腦或電子郵件的密碼無關；第二，只要公司有明確地宣示公司的監控政策或者是員工簽署同意公司監控的文件，員工在公司就不應該享有任何網路隱私的合理期待。這是目前社會所認同的看法，亦即員工在職場中沒有網路隱私權。

然而，隱私權係基於人性基本價值與基本尊嚴及人格發展之完整之基本權，

「為一個人生存所不可或缺且其核心為永久不可侵犯之權利」[186]，國家權力雖得以限制，但不容許全數侵害或是拋棄。同理可證，在私人公司的領域下，即便是公司提供的設備、監控政策的揭示、員工的同意等等的理由，也不能讓一個人將自身的隱私權全部放棄，這樣視同拋棄了自我的人性尊嚴，使憲法上基本權保護的功能變得空洞化，在一個民主自治的國家中，這樣破壞憲法基本精神的事情應不被允許[187]。好比員工即使使用了公司提供的文具寫信，並不表示公司可任意檢查其信件；公司提供抽屜，或提供制服、更衣間，但也不代表其可隨意抽查抽屜，或者是要求員工脫衣等行為，使用網路當然也是一樣的情況，特別是如果公司要求員工設定電腦、電子郵件的密碼時，員工自然更可以對此享有一定合理的隱私期待。

如圖 4-2 所述，員工對於保密規則的認知實際上只佔有一小部分，就算保密規則對員工具有拘束力，但就公司實際監控範圍遠大於員工所知的情況下，針對員工不知的部分仍應享有隱私的合理期待，亦即員工在職場中仍得擁有網路隱私權。

第二項　公司財產權與員工隱私權之基本權權利衝突

員工在公司裡使用的所有設備都是由公司所提供的，換言之，這些設備的所有權都屬於公司，因此在訪談中，有的主管曾經提到設備都是公司的財產，利用公司財產進行私人事務的處理，本來就不是正確的事[188]。而且營業秘密法規定公司需盡一切努力來保護營業秘密，其亦屬於公司的財產權[189]，藉以監控員工電子郵件及網路使用，亦即員工之網路隱私權來達成此目的，係為公司財產權與員工隱私權之「基本權第三人效力」的問題[190]所涉及之基本權權利衝突。

所謂「基本權第三人效力」，學說與實務上之通說為間接適用說[191]，此說認為基本權雖然屬於公權利，但其保障為憲法的基本價值決定，並具有強制規範的效力。因此對基本權之尊重亦為一種「公共秩序」或「善良風俗」，法律行為若對基本權造成侵害時，即背於「公序良俗」，應屬無效之法律行為。有鑑於此，即便基本權雖不能直接適用於民事關係，但仍可透過民事法上一般條款的適用，使基本

[186] 李惠宗，《憲法要義》，頁 83，元照(2001)。
[187] 基本權核心理論所保障的是憲法秩序之主體本身存在的價值，亦即人性尊嚴。陳慈陽，《憲法規範性與憲政現實性論文集》，頁 118-119，翰蘆(1997)。
[188] A3-2、A4-2 的訪談紀錄。
[189] 財產權之主題不限於自然人，包括法人，亦兼及非法人團體。請參見前註 186，頁 248。
[190] 基本權第三人效力之問題，使得基本權之理論不限於只適用在人民與國家之垂直方向，亦可能適用到人民與人民之間的水平方向。請參見前註 186，頁 103。
[191] 李惠宗，《權利分立與基本權保障》，頁 273-275，韋伯文化(1999)。亦可參見前註 186，頁 103。

權可間接適用於民事關係—當事人處於私法關係時，若其契約條款或特定法律行為已經造成基本權之侵害，可以違反公序良俗作為主張[192]。特別在私法關係上，不是一方全有或全無基本權的狀態，而是雙方皆有基本權，行使的結果造成其權利衝突[193]。

談到基本權權利衝突，大法官釋字第五零九號蘇俊雄大法官於協同意見書中第二段指出基本權之衝突問題，並提供解決之道：

「憲法保障的不同基本權之間，有時在具體事件中會發生基本權衝突－亦即，一個基本權主體在行使其權利時，會影響到另一個基本權主體的基本權利實現。基本權利之間發生衝突時，也就是有兩種看起來對立的憲法要求 (對不同基本權的實現要求) 同時存在；此時，必然有一方之權利主張必須退讓，方能維持憲法價值秩序的內部和諧。由於憲法所揭示的各種基本權，並沒有特定權利必然優先於另外一種權利的抽象位階關係存在，故在發生基本權衝突的情形時，就必須而且也只能透過進一步的價值衡量，來探求超越憲法對個別基本權保護要求的整體價值秩序。

就此，立法者應有「優先權限」(Vorrang) 採取適當之規範與手段，於衡量特定社會行為態樣中相衝突權利的比重後，決定系爭情形中對立基本權利實現的先後。而釋憲者的職權，則在於透過比例原則等價值衡量方法，審查現行規範是否對於相衝突的基本權利，已依其在憲法價值上之重要性與因法律規定而可能有的限制程度做出適當的衡量，而不至於過份限制或忽略了某一項基本權。至於在個案適用法律時，行政或司法機關亦應具體衡量案件中法律欲保護的法益與相對的基本權限制，據以決定系爭法律的解釋適用，追求個案中相衝突之基本權的最適調和」。

由此可知，當公司財產權與員工網路隱私權之基本權權利衝突時，應先進行**基本權之利益衡量**，而其衡量基準有三種方式[194]：一、基本權價值位序的衡量：此為將基本權定出有價值位序高低的作法，係「從國家總體價秩序，例如民主秩序、法治原則以及各基本權旨再促使個人基本尊嚴獲得確保的意旨」[195]來決定基本權的價值位序；二、手段的衡量：基本權利主體在行使基本權時，動機、目的為何及其採取何種手段。可歸納為 1.手段的適正性，亦即行使基本權之動機與目

[192] 請參見前註 186，頁 103。
[193] 請參見前註 191，頁 275。
[194] 請參見前揭註，頁 280-284。
[195] 請參見前揭註，頁 377-378。

的是否純正；2.手段比例性的衡量，係指出比例原則的適用；三、目的取向衡量：進行利益衡量時，不可違反立法目的，避免侵害權利主體之基本權。根據訪談結果可得知，目前公司為了避免財產權(特別指公司的營業秘密)受到侵害，對於員工的電子郵件及網際網路使用係採取全面性的監控，此種做法已經使員工網路隱私權蕩然無存，以手段衡量的標準來看，此已過度擴張行使公司財產權的基本權利，應依「比例原則」[196]來適度限制公司監控政策的手段。

欲應用比例原則於公司監控政策之檢視，需符合三項規定[197]，即適當性原則、必要性原則、以及過度禁止原則[198]。此三項原則指出在利益衡量下，公司監控員工電子郵件及網路使用的政策時，首先需合乎一定目的，且屬必要、侵害最小之手段，才能對員工進行監控，也就是說在針對營業秘密保護的目的下，公司應該以於業務上相關並特定的監控時間、範圍，並選擇對員工網路隱私權侵害最小的監控手段。這點是法院在審理這類案件時，所應該考慮的要點，只有避免公司因維護財產權而過分限制員工的網路隱私權，才能降低這兩項權利的衝突，以達到基本權利之調和。

除了利用基本權第三人效力之間接適用說之理論，將公司內部的監控現況與員工網路隱私權之衝突，利用利益衡量的方式取得兩私法關係上之主體之基本權衡平外，民法在八十八年修正後已將隱私權明定在條文中，為民法可主張的一種權利。因此亦可基於此說，間接適用民法之規定，員工應可以透過民法總則篇第七十二條：「法律行為，有背於公共秩序或善良風俗者，無效」，或者是第一百四十八條：「權利之行使，不得違反公共利益，或以損害他人為主要目的。行使權利，履行義務，應依誠實及信用方法」主張自己之網路隱私權，來避免公司在行使維護財產權的手段時，對員工電子郵件或網際網路使用的過度限制或監控，以員工網路隱私權所受到的侵害可能已經違反民法上公序良俗或權利濫用的規定，這是值得法院及立法者好好思索的另一個方向。

第三項　公司內針對員工網路隱私權之限制

196 比例原則早先係針對公權力對私人侵害時始有適用，旨在抑制國家權力之濫用，是否可適用於私法關係，仍有探討之空間。但有學者認為，比例原則為一「理性之行為準則」，在不能為了達到目的而不擇手段的宗旨下，於私法關係應有所適用，甚至違反比例原則的私法行為應即屬違法，國家公權力即可憑此介入私法關係。請參見前註 186，頁 117。

197 行政程序法亦有判斷比例原則程序之規定，於第七條：「行政行為，應依下列原則為之：一、採取之方法應有助於目的之達成。二、有多種同樣能達成目的之方法時，應選擇對人民權益損害最少者。三、採取之方法所造成之損害不得與欲達成目的之利益顯失均衡」。

198 請參見前註 186，頁 112-114。

第一款　保密規則是否可拘束員工的隱私權

保密規則應係屬工作規則內容之一部分，係按最高法院八十八年度台上字第一六九六號的判決理由：「…按在現代勞務關係中，因企業之規模漸趨龐大受僱人數超過一定比例者，僱主為提高人事行政管理之效率，節省成本有效從事市場競爭，就工作場所、內容、方式等應注意事項，及受僱人之差勤、退休、撫恤及資遣等各種工作條件，通常訂有共通適用之規範，俾受僱人一體遵循，此規範即工作規則。**勞工與雇主間之勞動條件依工作規則之內容而定，有拘束勞工與雇主雙方之效力，而不論勞工是否知悉工作規則之存在及其內容，或是否予以同意，除該工作規則違反法律強制規定或團體協商外，當然成為僱傭契約內容之一部。**雇主就工作規則為不利勞工之變更時，原則上不能拘束表示反對之勞工；但其變更具有合理性時，則可拘束表示反對之勞工…」以及九十一年度台上字第一六二五號：「…按**工作規則為雇主統一勞動條件及工作紀律，單方制定之定型化規則。雇主公開揭示時，係欲使其成為僱傭契約之附合契約，而得拘束勞雇雙方之意思表示。**勞工知悉後如繼續為該雇主提供勞務，應認係默示承諾該工作規則內容，而使該規則發生附合契約之效力。…」的見解。

根據以上兩判決之內容，工作規則除非違反法律強制規定，否則當然成為僱傭契約之附合契約，因此針對公司監控電子郵件及網路使用的政策亦即保密規則的內容，只要有適當的公開揭示，不論員工是否知悉其存在或內容，或是否給予同意，均有拘束員工的效力。

然而，針對保密規則的效力是否可拘束員工的網路隱私權，不無疑問。即便其係屬僱傭契約之一部分，私法上的契約是否足以限制憲法上的基本權，法院應作更清楚的解釋，立法者也應該深思這個問題。在李惠宗老師的書中提到，德國聯邦法院在「保證契約內容之審查案」認為，固然是契約自由，但是如果訂約其中一方具有單方面決定契約內容的強大地位，以致他方不容置喙、抑或造成顯失公平的情形時，民事法規應加以規範並使此契約有修正之可能[199]。

公司與員工，處於資方、勞方的不平等地位，當保密規則的內容包含監控員工電子郵件及網路使用的政策，對身為勞方的員工造成極大的限制，而員工也無法拒絕或改變這樣的政策時，在利益衡量上兩者已顯不相當，法院實不得因「契約就是契約」為由，不先審查 1.契約內含之工作規則的合理性及 2.國內相關隱私權保護的法規，而逕行拒絕員工。員工之所以針對公司監控電子郵件及網路使用的政策不聞不問，係因無法律約束公司的手段及範圍，也沒有任何救濟方式可以

[199] 請參見前註 191，頁 281-282。

幫助員工，如果發生糾紛員工根本求助無門，因此多數員工選擇忽略自己的網路隱私權，只願求得一份溫飽的工作，這是法院及立法者應好好思索的關鍵。

第二款　「同意」是否可完全排除隱私權

從訪談可得知，目前公司的做法都是公告監控電子郵件及網路使用政策的範圍模糊，員工只知道概括性的規範，資訊部門卻以員工完全不知道的手段、方法在全面監控員工的一舉一動，在這樣的情況下，如仍以員工明示或默示的同意來決定公司內是否具有合理的隱私期待，未免將公司財產權保護過分擴大。而且按前述法院見解，此保密規則只要有適當的公開揭示，員工是否知情、也根本不需要其同意，就能產生拘束員工的效力。既然如此，公司監控員工電子郵件及網路使用的政策根本不需員工的同意即可生效，那麼，員工的「同意」又何需討論？

就現況來看，同意的確降低了員工在公司內的隱私期待，但不代表著員工對自己隱私權的放棄，舉例來說，公司給予員工在公司內使用的不只是電腦、網路、電子郵件，還有辦公桌及衣櫃，難道公司就可以以業務目的之由，隨時搜查抽屜或櫃子內部的物品嗎？如果員工的同意是針對「公司業務上的監控」，而且認為只會受到機器設定關鍵字的搜尋，公司監控的政策如果超出這個範圍，那麼員工的同意還是有效的嗎？

筆者認為，針對公司監控員工電子郵件和網路使用並加以限制其網路隱私權的政策，不能僅有目的性地宣示，至少要 1.明確且完整地揭露監控政策的時間、內容與範圍，並且 2.讓員工清楚且瞭解公司的監控政策，在這種情況之下，員工的同意才可能為一有效之同意。而同意的形式為明示或默示，應仍以員工是否有一明確的意思表示為準，「不反對即表示同意」的想法不應該被認可，誠如前所述，勞資雙方地位的不對等，造成員工沒有辦法拒絕公司的監控政策，且在沒有法律的規範下，員工亦沒有申訴的機會。既然如此，員工在對公司監控政策的完全瞭解下，明確地表達同意係為一同意公司監控其使用電子郵件及網路的當然要件，但是，**此等同意也只是減少員工在職場中合理的隱私期待而已，並不代表著員工在工作場合中完全放棄自己的網路隱私權。**這點對於沒有法律明文規定且採取企業自治的我國現況，實在是迫切需要透過法院解釋之重點。

第四項　其他

資訊部門在公司裡的地位是相當高的，除了負責管理公司內部的網絡系統之外，還身兼保密規則內容的制定，決定監控的手段，以及負責監控全公司的電腦

使用情形，將違規的員工隨時報以其主管。此同時身兼行政、立法、司法的地位，公正性自然會受到質疑，針對資訊部門，在訪談時，被訪談者 A5-2 曾提到：對資訊部門的員工，最後公司的選擇就是「信任」，只有真正重要的機密，會以監控器紀錄及一台鎖在機櫃的電腦，在主任的陪同下，才能進行查閱的動作。由此可知，全公司的資料流通都會在資訊部門留下紀錄，而這些紀錄不論基於業務或非業務上的目的傳送，都有機會被監看，這樣反而造成資訊部門成為了最有監控能力，但也是最有洩密能力的部門，此時誰來監控這些監控者？

保密規則的制定，包含決定公司資訊流通的方向以及監控的手段，前者來說，資訊部門的員工在管理上似乎常常沒有一個標準，被訪談者 A5-1 曾反應過自己部門何以較另一掌握較多資訊的部門網路管制較嚴格，而且很多事情在通過層層保密關卡後，無法即時完成，這對瞬息萬變的科技業是很大的傷害。這透露出一個訊息，員工根本不明白針對不同部門、不同開放網路權限的標準在哪？而且管制的目的係為了維護公司機密，另一部分則是希望提高員工工作績效，但是當公司資訊流通過度管制時，反而很有可能造成工作效率低落，係與當初管制目的不合。以後者而言，監控使用的手段、範圍，監控的時間，亦由資訊部門決定要公開多少內容給員工知道，在無法可管的情形下，資訊部門擁有極大的裁量權，將來很有機會以保護公司營業秘密為由，進而作出更多、更全面性，而員工完全不知道的網路監控，而這是多數學者的文章並未提到之處。

第三節　小結

財產權與隱私權之基本權的保障，皆是人性尊嚴與人格發展自由的保障，需利用基本權第三人效力理論，將基本權間接適用於私法關係。不過若以憲法基本權價值位序原則，很難分出一個高下。而公司財產權與員工網路隱私權之基本權權利衝突是一個十分難解的問題，但也並非完全沒有解決的答案，在現今公司內進行全面性監控，而員工只知道一部分的政策的情況，很明顯地已經違反了比例原則。法院與立法者應深思勞資雙方的地位不對等的關鍵，除了以隱私的合理期待作為考量這類案件的先決條件外，應透過解釋或立法規範，利用比例原則盡量達到這兩項基本權利的衡平，抑或是利用民法總則篇公序良俗或權利不可濫用之規定，嘗試為公司監控的範圍與員工網路隱私權之間畫出一條界限。

以隱私的合理期待作為考量重點，應針對保密規則及監控政策內容之合理性以及員工同意時之情形進行審酌，前者雖以最高法院八十八年度台上字第一六九六號、九十一年度台上字第一六二五號得到工作規則視為勞動契約之一部的結論，根本上否定了員工表達意見的權利，然而對於契約的合理性仍應有討論的空

間；後者的同意並不代表對自己隱私權的全面放棄，而是公司應清楚、完整揭示所有監控電子郵件及網際網路使用的政策，在員工確實明白、了解後，以一明確的意思表示表達其同意，此同意才能為法律上一有效的同意。若超過此同意範圍所為之的監控，應視為已經侵害員工的網路隱私權，法院不應以其為工作規則，員工不需知悉或同意而逕行拘束員工或認為員工喪失對職場中隱私的合理期待。最重要的是，即便是公司的設備全為公司所有、監控政策已公開揭示、員工同意此政策等之情況，仍不等於員工網路隱私權之拋棄，員工在職場中仍應享有一定的隱私期待，隱私權係為人性尊嚴及基本價值之基本權，不得任意捨棄而破壞民主法治國家之憲法基本精神。

又，公司的資安部門掌握極大資訊流通與控制的權利，在其過度管制下，繁複的把關手續反而造成員工工作效率低落，也許透過立法管制，建立一套標準的審核，讓員工不會無所適從或擔心資訊的洩漏，這也是另一個思考的方向。

第六章　結論與建議

第一節　結論

科技進步，資訊快速流通，電子郵件及網際網路的使用已經成為了生活或工作不可或缺的一部分，然而公司的員工在享受這樣便利的同時，亦受到公司的監控，沒有任何私人空間與秘密。而根據本論文對新竹科學園區公司的員工進行深度訪談的研究結果，可得出以下結論：

一、很顯然地，公司監控員工電子郵件及網路使用之情形，已經涉及憲法上公司財產權與員工網路隱私權之基本權權利衝突，其手段、範圍已經違反憲法上的比例原則。

二、政府目前對這類事件採取企業自治的態度，法院判決(最高法院八十八年度台上字第一六九六號、九十一年度台上字第一六二五號針對工作規則的認定、台北地方法院九十一年度勞訴字第一三九號對於隱私的合理期待的推論)係傾向資方，亦即公司。

三、公司監控員工電子郵件及網路使用的情形沒有法律明文規範，即使今天科技技術面可以達到特定時間、目的的監控，而且事實上公司內部資料多半有分級制度[200]，但是決策者仍在於人，因此員工多半缺乏認識或漠不關心，即便網路隱私權被侵害仍無法察覺或自力救濟。

四、這類事件不乏有新聞報導[201]，但是法院判決卻很少，唯一的判決甚至不是出現新竹地方法院，可約略推知面對這類事件，新竹科學園區的公司多數不尋求司法途徑解決，僅以私下開除員工抑或是警告作為懲處的方式，這樣的處理模式，可避免洩密和公司競爭對手的攻擊。換個角度想，如果員工可以透過法律規定進行網路隱私權侵害的救濟，或許法院就會開始正視這樣的管理方式是否妥當合宜，仔細審視目前公司內部的保密規則與監控政策的內容，進一步追求兩相衝突的公司財產權與員工網路隱私權之基本權的最適調和。

---

[200] 根據訪談紀錄，有幾家公司針對公司內部流通的資料設有分級制度，多數分成三級，也有的公司分成四級，甚至連內部資訊及公司財產都算是保密層級之一，而不得對外洩漏。例如：保密規則亦屬公司內部資訊，因此不得對外洩漏。請參見第四章第二節。

[201] 請參見第一章緒論。

五、公司內部電子郵件或網路使用的過度管制，反而在公司運作機制上造成了阻礙，導致員工工作效率低落。另一方面，員工不知道制定規則的資訊部門的標準，也不清楚自己的個人資料是否有外洩之可能，在層層把關之下，很有可能增加員工的心理壓力，反降低其工作效率，與當初管制目的所欲達成之提高員工工作績效(此亦為了追求公司利益)，似有所矛盾。

第二節　建議

基於勞資雙方的地位並不對等，目前公司監控員工電子郵件及網際網路使用的政策，已不足單以企業自治作為合法管理的依據。筆者建議，這種非明顯可知的網路隱私侵害，員工無法及時警覺，甚至缺乏認識，抑或是無力自行救濟，政府應該伸出援手，不該以少數的幾條規定來適用多數場合的監控行為，而且法院也應針對網路的隱私侵害有更多的認識，避免判決傾向資方，而不對其侵害的內容作出更仔細的判斷與審視。

立法管制最重要的目的應使公司監控政策完全透明化，並合乎比例原則，可以讓員工有選擇及同意的權利，可參酌第三章第四節歐盟於二零零二年五月公佈的工作報告的內容[202]，或至少要讓公司監控員工電子郵件及網際網路使用的政策符合以下幾項要求[203]：「

一、基於合法上的業務上的目的；

二、使用最小侵害手段來達到業務上的目標；

三、讓接近、使用以及揭露資訊限制在足以達成目的的範圍之內；

四、提供合理的通知已告知員工監視及使用的情形」，

根據這四點原則作為立法上的參考，立法內容應包含公司監控的時間、範圍、手段皆需特定化，透過制度設計訂出明確的界限，並盡量避免完全可規避之例外情形，讓公司沒有機會迴避這樣的責任。

---

[202] 請參見本論文第三章第四節有關歐盟提出之工作報告內容，其針對工作場合中電子通訊之監控須符合七項原則之說明，

[203] Laurie Thomas Lee, *Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop"*, 28 J. Marshall L. Rev. 139 (1994). 另請參見王郁琦，前註 113，頁 104-105。

筆者認為立法者應規範公司的政策需明確，不能僅有例示性的宣示，**最重要的是必須提供員工申訴的管道或救濟的途徑**，公司與員工才會更加重視這個問題。立法雖迫切，但立法前透過法院解釋也可以暫時彌補這一部分的缺憾—在公司網路監控政策與侵犯員工網路隱私權之間利用民事法規之適用，盡量劃一條清楚的界線。而法院與立法者最應了解的關鍵仍是在於僱傭契約與工作規則係公司具有一單方面決定契約內容的強大地位，不該為了成就一方的利益，而完全犧牲了另一方的權利，也因此，才需要政府公權力的介入。

第三節　後續研究建議

本文所提到的公司監控員工電子郵件及網際網路使用的政策，僅是公司監控的冰山一角，訪談中可得知員工身上掛的門禁卡，儲存著許多個人資訊，如果想要調查員工一天的行程，實非難事，因為各辦公室、實驗室、餐廳，以及健康檢查的結果，甚至使用幾次印表機、影印機、內容為何等，都會透過這張卡連線到公司主機，進行檢視[204]，那麼，這跟過去政府欲發行「國民身分健保合一智慧卡」(簡稱國民卡)的政策所牽涉的法律爭議有何不同？筆者認為這仍有討論之空間。

另外，資訊部門在公司的地位、其監控者身分的討論以及監控的標準，是否也需要透過立法管制，成為另一個可以思考的方向。

其實，有關公司監控員工電子郵件及網際網路使用的政策，已經涉及了相關勞工權益的議題，應可從勞工法方面進行另一方向的探究。也可透過美國法院適用 ECPA 三項例外規定的這類判決之統計，進行分析，惟此部分不在本論文討論範圍之內，但仍可資未來相關研究者之參考。

[204] 舉例來說，被訪談者 A5-1 就曾經因兩天的中餐吃了炸雞類的食物，結果公司的健康中心寄來一封電子郵件，提醒其不該吃這類食品，因其上次健康檢查的資料顯示其身體有高血壓及三酸甘油脂數值偏高的狀況，這似乎在告訴員工，其健康情形也成為了一種公司無形的財產；或者是藉節能減碳之名，實際上則是為了減少公司成本，公司物品藉由刷卡領取，包含文具用品、衛生紙等，亦可了解每一個員工的支出及在公司的行為。

參考文獻

英文書籍

1. DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE (2001).
2. J. THOMAS MCCARTHY, THE RIGHT OF PUBLICITY AND PRIVACY (2008).
3. KURT H. DECKER, A MANAGER'S GUIDE TO EMPLOYEE PRIVACY: LAWS, POLICES, AND PROCEDURES (1989).
4. KURT H. DECKER, DRAFTING AND REVISING EMPLOYMENT POLICES AND HANDBOOKS (2nd ed. 1994).
5. MICHAEL ROGERS RUBIN, PRIVATE RIGHTS, PUBLIC WRONGS: THE COMPUTER AND PERSONAL PRIVACY (1988).
6. ONLINE (Thomas F. Smedinghoff ed., 1996).
7. PAUL M. SCHWARTZ, JOEL R. REIDENBERG, DATA PRIVACY LAW (1996).
8. SURVEILLANCE AS SOCIETY SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION (David Lyon ed., 2003).

中文書籍

1. David Brin 著，蕭美惠譯，《透明社會─個人隱私 v.s.資訊自由》，先覺(1999)。
2. Earl Babbie 著，陳文俊譯，《社會科學研究方法》，雙葉書廊(2005)。
3. Ellen Alderman, Caroline Kennedy 著，吳懿婷譯，《隱私的權利》，城邦文化(2001)。
4. Ranjit Kumar 著，胡龍騰、黃瑋瑩、潘中道譯，《研究方法：步驟化學習指南》，學富文化(2002)。
5. Thomas Herzog 著，朱柔若譯，《社會科學研究方法與資料分析》，揚智文化(1996)。
6. W.Lawrence Neuman 著，王佳煌、潘中道、郭俊賢、黃瑋瑩譯，《當代社會研究法─質化與量化途徑》，學富文化(2002)。
7. 王郁琦，《資訊、電信與法律》，元照(2004)。
8. 石之瑜，《社會科學方法新論》，五南圖書(2003)。
9. 李惠宗，《權利分立與基本權保障》，韋伯文化(1999)。
10. 李惠宗，《憲法要義》，元照(2001)。
11. 李念祖，《案例憲法Ⅲ(上)─人權保障的內容》，三民書局(2006)。
12. 林山田，《刑法各罪論上冊》，自刊(修訂三版，2002)。
13. 錢世傑，《獵殺隱私時代─10 個讓你失去隱私的理由》，三民書局(2004)。

英文期刊論文

1. A. Micheal Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000).
2. Corey A. Ciocchetti, *Monitoring Employee E-mail: Efficient Workplaces vs. Employee Private*, 2001 DUKE L. & TECH. REV. 26 (2001).
3. Daniel Benoliel, *Law, Geography and Cyberspace: The Case of On-line Territorial Privacy*, 23 CARDOZO ARTS & ENT. L.J. 125 (2005).
4. Kevin P. Kopp, *Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy*, 8 SETON HALL CONST. L.J. 861 (1998).
5. Laurie Thomas Lee, *Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop"*, 28 J. MARSHALL L. REV. 139 (1994).
6. Marc-Alexandre Poirier, *Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?*, 60 U. TORONTO FAC. L. REV. 85 (2002).
7. S. Elizabeth Wilborn, R*evisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825 (1998).
8. Sarah DiLuzio, *Workplace E-mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741 (2000).

中文期刊論文

1. H. Thomas Davis，黃河譯，〈網路法律：監控員工的電子通訊〉，《網路資訊》，五月號(2001)。
2. 王郁琦，〈網路上的隱私權問題〉，《資訊法務透析》，十月號(1999)。
3. 吳兆琰，〈從國內外實務見解談企業對員工之電子郵件監控〉，《科技法律透析》，第十六卷第十期(2004)。
4. 李震山，〈資訊時代下「資訊權」入憲之芻議〉，《律師雜誌》，第三零七期(2005)。
5. 范姜真媺，〈企業內電子郵件之監看與員工隱私權〉，《臺灣本土法學雜誌》，第六十期(2004)。
6. 陳仲嶙、賴文智，〈職場電子郵件監視的隱私權問題〉，《網路資訊》，二月號(2001)。
7. 馮震宇，〈企業 E 化的新挑戰—企業權益與員工隱私權保護的兩難與調和〉，《月旦法學雜誌》，第八十五期(2002)。
8. 黃程貫，〈雇主監看員工電子郵件之合法界限—台北地院九一年勞訴字第一三九號民事判決評釋〉，《臺灣本土法學雜誌》，第七十三期(2005)。
9. 詹文凱，〈美國法上個人資訊隱私權的相關判決〉，《律師雜誌》，第二三三期(1999)。

10. 劉靜怡，〈資訊科技與隱私權焦慮—誰有權塑造我的網路形象〉，《當代雜誌》，第一二四期(1997)。
11. 劉定基，〈資訊時代的職場隱私權保護—以台北地院九十一年度勞訴字第一三九號判決為中心〉，《律師雜誌》，第三零七期(2005)。
12. 簡榮宗，〈監看員工電子郵件產生的隱私權爭議〉，《全國律師》，第六卷第五期(2002)。

中文學位論文

1. 邱惠雯，〈網際網路使用行為之限制─從隱私權保護觀之探討〉，國立中正大學犯罪防治研究所碩士論文(2003)。
2. 徐新隆，〈數位時代下資訊隱私權問題之研究─以個人資料保護為中心〉，國立台北大學法律學系研究所碩士論文(2005)。
3. 詹文凱，〈隱私權之研究〉，國立臺灣大學法律學研究所博士論文(1998)。
4. 錢世傑，〈網路通訊監察法制與相關問題研究〉，中原大學財經法律研究所(2001)
5. 簡榮宗，〈網路上資訊隱私權保護問題之研究〉，東吳大學法律學系研究所碩士論文(2000)。

其他文獻資料

1. 月旦法學知識庫：http://www.lawdata.com.tw
2. 司法院法學檢索系統：http://nwjirs.judicial.gov.tw/Index.htm
3. 全國法規資料庫：http://law.moj.gov.tw/fn/fn-c.asp
4. 行政院主計處：http://www.dgbas.gov.tw
5. 法源法律網：http://www.lawbank.com.tw/index.php
6. 國家圖書館--全國博碩士論文資訊網：http://etds.ncl.edu.tw/theabs/index.jsp
7. American management association：http://www.amanet.org
8. DUKE law & technology REVIEW：http://www.law.duke.edu/journals/dltr/
9. Electronic Privacy Information Center：http://epic.org/
10. FINDLAW：http://www.findlaw.com/
11. Library of Congress：http://www.loc.gov/index.html
12. International Labour Organization：http://www.ilo.org/global/lang--en/index.htm
13. Privacy Law Blog：http://privacylaw.proskauer.com
14. The European Union：http://europa.eu/index_en.htm
15. WESTLAW：http://international.westlaw.com

附錄一　通訊保障及監察法 (民國 96 年 7 月 11 日修正)

【資料來源：全國法規資料庫<http://law.moj.gov.tw/fn/fn-c.asp>】

第 1 條　為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序，特制定本法。

第 2 條　通訊監察，除為確保國家安全、維持社會秩序所必要者外，不得為之。

前項監察，不得逾越所欲達成目的之必要限度，且應以侵害最少之適當方法為之。

第 3 條　本法所稱通訊如下：

一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。

二、郵件及書信。

三、言論及談話。

前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。

第 4 條　本法所稱受監察人，除第五條及第七條所規定者外，並包括為其發送、傳達、收受通訊或提供通訊器材、處所之人。

第 5 條　有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。

一、最輕本刑為三年以上有期徒刑之罪。

二、刑法第一百條第二項之預備內亂罪、第一百零一條第二項之預備暴動內亂罪或第一百零六條第三項、第一百零九條第一項、第三項、第四項、第一百二十一條第一項、第一百二十二條第三項、第一百三十一條第一項、第一百四十二條、第一百四十三條第一項、第一百四十四條、第一百四十五條、第二百零一條之一、第二百五十六條第一項、第三項、第二百五十七條第一項、第四項、第二百九十八條第二項、第三百條、第三百三十九條、第三百三十九條之三或第三百四十六條之罪。

三、貪污治罪條例第十一條第一項、第二項之罪。

四、懲治走私條例第二條第一項、第三項或第三條之罪。

五、藥事法第八十二條第一項、第三項或第八十三條第一項、第四項之罪。

六、證券交易法第一百七十一條或第一百七十三條第一項之罪。

七、期貨交易法第一百十二條或第一百十三條第一項、第二項之罪。

八、槍砲彈藥刀械管制條例第十二條第一項、第二項、第四項、第五項或第十三條第二項、第四項、第五項之罪。

九、公職人員選舉罷免法第八十八條第一項、第八十九條第一項、第二

項、第九十條之一第一項、第九十一條第一項第一款或第九十一條之一第一項之罪。
十、農會法第四十七條之一或第四十七條之二之罪。
十一、漁會法第五十條之一或第五十條之二之罪。
十二、兒童及少年性交易防制條例第二十三條第一項、第四項、第五項之罪。
十三、洗錢防制法第九條第一項、第二項之罪。
十四、組織犯罪防制條例第三條第一項後段、第二項後段、第六條或第十一條第三項之罪。
十五、陸海空軍刑法第十四條第二項、第十七條第三項、第十八條第三項、第十九條第三項、第二十條第五項、第二十二條第四項、第二十三條第三項、第二十四條第二項、第四項、第五十八條第五項、第六十三條第一項之罪。
前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權以書面記載第十一條之事項，並敘明理由、檢附相關文件，聲請該管法院核發；檢察官受理申請案件，應於二小時內核復。如案情複雜，得經檢察長同意延長二小時。法院於接獲檢察官核轉受理申請案件，應於二十四小時內核復。審判中由法官依職權核發。法官並得於通訊監察書上對執行人員為適當之指示。
前項之聲請經法院駁回者，不得聲明不服。
執行機關應於執行監聽期間，至少作成一次以上之報告書，說明監聽行為之進行情形，以及有無繼續執行監聽之需要。法官依據經驗法則、論理法則自由心證判斷後，發現有不應繼續執行監聽之情狀時，應撤銷原核發之通訊監察書。
違反本條規定進行監聽行為情節重大者，所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據。

第 6 條 有事實足認被告或犯罪嫌疑人有犯刑法妨害投票罪章、公職人員選舉罷免法、總統副總統選舉罷免法、槍砲彈藥刀械管制條例第七條、第八條、毒品危害防制條例第四條、擄人勒贖罪或以投置炸彈、爆裂物或投放毒物方法犯恐嚇取財罪、組織犯罪條例第三條、洗錢防制法第十一條第一項、第二項、第三項、刑法第二百二十二條、第二百二十六條、第二百七十一條、第三百二十五條、第三百二十六條、第三百二十八條、第三百三十條、第三百三十二條及第三百三十九條，為防止他人生命、身體、財產之急迫危險，司法警察機關得報請該管檢察官以口頭通知執行機關先予執行通訊監察。但檢察官應告知執行機關第十一條所定之事項，並於二十四小時內陳報該管法院補發通訊監察書；檢察機關為受理緊急監察案件，應指定專責主任檢察官或檢察官作為緊急聯繫窗口，以

利掌握偵辦時效。

法院應設置專責窗口受理前項聲請，並應於四十八小時內補發通訊監察書；未於四十八小時內補發者，應即停止監察。

違反本條規定進行監聽行為情節重大者，所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據。

第 7 條 為避免國家安全遭受危害，而有監察下列通訊，以蒐集外國勢力或境外敵對勢力情報之必要者，綜理國家情報工作機關首長得核發通訊監察書。

一、外國勢力、境外敵對勢力或其工作人員在境內之通訊。

二、外國勢力、境外敵對勢力或其工作人員跨境之通訊。

三、外國勢力、境外敵對勢力或其工作人員在境外之通訊。

前項各款通訊之受監察人在境內設有戶籍者，其通訊監察書之核發，應先經綜理國家情報工作機關所在地之高等法院專責法官同意。但情況急迫者不在此限。

前項但書情形，綜理國家情報工作機關應即將通訊監察書核發情形，通知綜理國家情報工作機關所在地之高等法院之專責法官補行同意；其未在四十八小時內獲得同意者，應即停止監察。

違反前二項規定進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據。

第 8 條 前條第一項所稱外國勢力或境外敵對勢力如下：

一、外國政府、外國或境外政治實體或其所屬機關或代表機構。

二、由外國政府、外國或境外政治實體指揮或控制之組織。

三、以從事國際或跨境恐怖活動為宗旨之組織。

第 9 條 第七條第一項所稱外國勢力或境外敵對勢力工作人員如下：

一、為外國勢力或境外敵對勢力從事秘密情報蒐集活動或其他秘密情報活動，而有危害國家安全之虞，或教唆或幫助他人為之者。

二、為外國勢力或境外敵對勢力從事破壞行為或國際或跨境恐怖活動，或教唆或幫助他人為之者。

三、擔任外國勢力或境外敵對勢力之官員或受僱人或國際恐怖組織之成員者。

第 10 條 依第七條規定執行通訊監察所得資料，僅作為國家安全預警情報之用。但發現有第五條所定情事者，應將所得資料移送司法警察機關、司法機關或軍事審判機關依法處理。

第 11 條 通訊監察書應記載下列事項：

一、案由及涉嫌觸犯之法條。

二、監察對象。

三、監察通訊種類及號碼等足資識別之特徵。

四、受監察處所。

五、監察理由。

六、監察期間及方法。

七、聲請機關。

八、執行機關。

九、建置機關。

前項第八款之執行機關，指蒐集通訊內容之機關。第九款之建置機關，指單純提供通訊監察軟硬體設備而未接觸通訊內容之機關。

核發通訊監察書之程序，不公開之。

第 12 條 第五條、第六條之通訊監察期間，每次不得逾三十日，第七條之通訊監察期間，每次不得逾一年；其有繼續監察之必要者，應附具體理由，至遲於期間屆滿之二日前，提出聲請。

第五條、第六條之通訊監察期間屆滿前，偵查中檢察官、審判中法官認已無監察之必要者，應即停止監察。

第七條之通訊監察期間屆滿前，綜理國家情報工作機關首長認已無監察之必要者，應即停止監察。

第 13 條 通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。

執行通訊監察，除經依法處置者外，應維持通訊暢通。

第 14 條 通訊監察之執行機關及處所，得依聲請機關之聲請定之。法官依職權核發通訊監察書時，由核發人指定之；依第七條規定核發時，亦同。

電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。

前項因協助執行通訊監察所生之必要費用，於執行後，得請求執行機關支付；其項目及費額由交通部會商有關機關訂定公告之。

電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。

前項協助建置通訊監察系統所生之必要費用，由建置機關負擔。另因協助維持通訊監察功能正常作業所生之必要費用，由交通部會商有關機關訂定公告之。

第 15 條 第五條、第六條及第七條第二項通訊監察案件之執行機關於監察通訊結束時，應即敘明受監察人之姓名、住所或居所報由檢察官、綜理國家情報工作機關陳報法院通知受監察人。如認通知有妨害監察目的之虞或不能通知者，應一併陳報。

法院對於前項陳報，除認通知有妨害監察目的之虞或不能通知之情形外，應通知受監察人。

前項不通知之原因消滅後，執行機關應報由檢察官、綜理國家情報工作機關陳報法院補行通知。

關於執行機關陳報事項經法院審查後，交由司法事務官通知受監察人。

第 16 條 執行機關於監察通訊後，應按月向檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長報告執行情形。檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長並得隨時命執行機關提出報告。

第五條、第六條通訊監察之監督，偵查中由檢察機關、審判中由法院，第七條通訊監察之監督，由綜理國家情報工作機關，派員至建置機關，或使用電子監督設備，監督通訊監察執行情形。偵查中案件，法院得隨時派員監督執行機關執行情形。

第 17 條 監察通訊所得資料，應加封緘或其他標識，由執行機關蓋印，保存完整真實，不得增、刪、變更，除已供案件證據之用留存於該案卷或為監察目的有必要長期留存者外，由執行機關於監察通訊結束後，保存五年，逾期予以銷燬。

通訊監察所得資料全部與監察目的無關者，執行機關應即報請檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長許可後銷燬之。

前二項之資料銷燬時，執行機關應記錄該通訊監察事實，並報請檢察官、依職權核發通訊監察書之法官或綜理國家情報工作機關首長派員在場。

第 18 條 依本法監察通訊所得資料，不得提供與其他機關（構）、團體或個人。但符合第五條或第七條之監察目的或其他法律另有規定者，不在此限。

第 19 條 違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，負損害賠償責任。

被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

前項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

第 20 條 前條之損害賠償總額，按其監察通訊日數，以每一受監察人每日新台幣一千元以上五千元以下計算。但能證明其所受之損害額高於該金額者，不在此限。

前項監察通訊日數不明者，以三十日計算。

第 21 條 損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者亦同。

第 22 條 公務員或受委託行使公權力之人，執行職務時違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，國家應負

損害賠償責任。

依前項規定請求國家賠償者，適用第十九條第二項、第三項及第二十條之規定。

第 23 條 損害賠償除依本法規定外，適用民法及國家賠償法規定。

第 24 條 違法監察他人通訊者，處五年以下有期徒刑。

執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。

意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。

第 25 條 明知為違法監察通訊所得之資料，而無故洩漏或交付之者，處三年以下有期徒刑。

意圖營利而犯前項之罪者，處六月以上五年以下有期徒刑。

第 26 條 前二條違法監察通訊所得之資料，不問屬於犯人與否，均沒收之。

犯人不明時，得單獨宣告沒收。

第 27 條 公務員或曾任公務員之人因職務知悉或持有依本法或其他法律之規定監察通訊所得應秘密之資料，而無故洩漏或交付之者，處三年以下有期徒刑。

第 28 條 非公務員因職務或業務知悉或持有依本法或其他法律之規定監察通訊所得應秘密之資料，而無故洩漏或交付之者，處二年以下有期徒刑、拘役或新台幣二萬元以下罰金。

第 29 條 監察他人之通訊，而有下列情形之一者，不罰：

一、依法律規定而為者。

二、電信事業或郵政機關（構）人員基於提供公共電信或郵政服務之目的，而依有關法令執行者。

三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。

第 30 條 第二十四條第一項、第二十五條第一項及第二十八條之罪，須告訴乃論。

第 31 條 有協助執行通訊監察義務之電信事業及郵政機關（構），違反第十四條第二項之規定者，由交通部處以新台幣五十萬元以上二百五十萬元以下罰鍰；經通知限期遵行而仍不遵行者，按日連續處罰，並得撤銷其特許或許可。

第 32 條 軍事審判機關於偵查、審判現役軍人犯罪時，其通訊監察準用本法之規定。

前項通訊監察書於偵查現役軍人犯罪時，由軍事檢察官向該管軍事審判官聲請核發。軍事審判官並得於通訊監察書上，對執行人員為適當之指示。

執行機關應於執行監聽期間，至少作成一次以上之報告書，說明監聽行

為之進行情形，以及有無繼續監聽之需要。軍事審判官依經驗法則、論理法則自由心證判斷後，發現有不應繼續執行監聽之情狀時，應撤銷原通訊監察書。

違反前三項規定進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據。

第 33 條　本法施行細則，由行政院會同司法院定之。

第 34 條　本法自公布日施行。

本法修正條文自公布後五個月施行。

附錄二　電子通訊隱私權法案

Electronic Communication Privacy Act

【資料來源：FINDLAW<http://www.findlaw.com/>】

United States Code

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE

PART I - CRIMES

CHAPTER 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Section 2510. Definitions

As used in this chapter -

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than –

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof,

(i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means –

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" has the meaning given that term in section 3 of the Communications Act of 1934;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include -

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who -

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not -

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means -

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means -

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against -

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a

foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to -

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser" -

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

Section 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who -

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when -

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use

(A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of he United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)

(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter,

(ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,

(iii) having obtained or received the information in connection with a criminal investigation, and

(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a)

(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign

Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with -

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for

the purpose of committing any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person -

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted -

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which -

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is

causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter -

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if -

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)

(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication -

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)

(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted -

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)

(a)

(i) If the communication is -

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection -

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be

entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

Section 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally -

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of -

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for -

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

Section 2513. Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to

(1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code,

(2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof,

(3) the remission or mitigation of such forfeiture,

(4) the compromise of claims, and

(5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

Section 2514. Repealed. Pub. L. 91-452, title II, Sec. 227(a), Oct. 15, 1970, 84 Stat. 930]

Section 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

Section 2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General,(!1) or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of -

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section

201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to

prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline) or section 46502 (relating to aircraft piracy) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);

(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications),

section 1546 (relating to fraud and misuse of visas, permits, and other documents) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or

(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2332f, 2339A, 2339B, or 2339C of this title (relating to terrorism); or

(r) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

Section 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the

disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying

out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

Section 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including

(i) details as to the particular offense that has been, is being, or is about to be

committed,

(ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted,

(iii) a particular description of the type of communications sought to be intercepted,

(iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that -

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that

offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify -

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law

enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that -

(a) an emergency situation exists that involves -

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has

occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)

(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice

of -

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted. The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)

(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that -

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval. Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted

communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if -

(a) in the case of an application with respect to the interception of an oral communication -

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication -

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception

only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

Section 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts -

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts -

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the

preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including

(i) the approximate nature and frequency of incriminating communications intercepted,

(ii) the approximate nature and frequency of other communications intercepted,

(iii) the approximate number of persons whose communications were intercepted,

(iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and

(v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

Section 2520. Recovery of civil damages authorized

(a) In General. - Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other

than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief. - In an action under this section, appropriate relief includes -

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of Damages. –

(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of -

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense. - A good faith reliance on -

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation. - A civil action under this section may not be commenced later than two

years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative Discipline. - If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper Disclosure Is Violation. - Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

Section 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

Section 2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) Enforcement by Court Issuing Surveillance Order. - If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier

has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) Enforcement Upon Application by Attorney General. – The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) Civil Penalty. -

(1) In general. - A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

(2) Considerations. - In determining whether to impose a civil penalty and in determining its amount, the court shall take into account -

(A) the nature, circumstances, and extent of the violation;

(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

(C) such other matters as justice may require.

(d) Definitions. - As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

AMENDMENTS

1994 - Pub. L. 103-414, title II, Sec. 201(b)(3), Oct. 25, 1994, 108 Stat. 4290, added item 2522.

1988 - Pub. L. 100-690, title VII, Sec. 7035, Nov. 18, 1988, 102 Stat. 4398, substituted "wire, oral, or electronic" for "wire or oral" in items 2511, 2512, 2513, 2516, 2517, 2518, and 2519.

1986 - Pub. L. 99-508, title I, Secs. 101(c)(2), 110(b), Oct. 21, 1986, 100 Stat. 1851, 1859, inserted "AND ELECTRONIC COMMUNICATIONS" in chapter

heading and added item 2521.

1970 - Pub. L. 91-452, title II, Sec. 227(b), Oct. 15, 1970, 84 Stat. 930, struck out item 2514 "Immunity of witnesses", which section was repealed four years following the sixtieth day after Oct. 15, 1970.

1968 - Pub. L. 90-351, title III, Sec. 802, June 19, 1968, 82 Stat. 212, added chapter 119 and items 2510 to 2520.

CHAPTER REFERRED TO IN OTHER SECTIONS

This chapter is referred to in sections 1029, 2232, 2712 of this title; title 47 sections 551, 605, 1008; title 50 section 1805.