第三章　企業內電子郵件監控的爭議－美國法的觀察

The law embodies the story of a nation's development through many centuries, and it cannot be dealt with as if it contained only the axioms and corollaries of a book of mathematics. In order to know what it is, we must know what it has been, and what it tends to become.--- Justice Oliver Wendell Holmes

第一節　概說

Warren 和 Brandeis教授於1890年，在題爲「隱私的權利」（The Right to Privacy）一文中指出：「新近的發明和商業手法使得人們開始注意到要更進一步提供對個人的保護。…獨處的權利」「現代企業和發明造成隱私侵犯的精神痛苦，遠比人身傷害大」[151]。並且提出警告「無數的機械設備預示著，將來有一天，我們在密室中的低語，將會如同在屋頂大聲宣告般」[152]。

一百多年後，「新近的發明」和「商業手法」與在19世紀所可理解的，已經大相逕庭。電腦科技和網際網路的發展，徹底爲工作場所帶來革命性的發展。

電子郵件成爲新的商業通訊方式。同時，電子郵件也是最流行的線上活動。至2003年，美國有百分之五十四點六的家庭接觸網際網路；有百分之八十七點八的網際網路用戶收發電子郵件[153]。現代工作場亦所爲電子郵件和電子工具所浸透。根據

[151] "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.'" "modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."

[152] "…and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

[153] United States Department of Commerce, Economics and Statistics Administration & National Telecommunications and Information Administration, A Nation Online: Entering the Broadband Age 9 (2004), available at

統計，在2000年，有四千萬名美國員工發送600億封電子郵件[154]。

然而，電腦科技也爲隱私帶來無比威脅，成爲雙刃的劍（double-edged sword）。電子郵件監看技術也成爲個人自決權的新對手。

根據美國管理協會（American Management Association, AMA ）的調查指出，在美國，約 45%的大型企業承認監看員工的電子郵件、電話、及電腦檔案內容，這個數字在 1998 年至 2000 年中，成長了一成左右。其中，電子郵件又是企業監看的「最愛」[155]。而到 2001 年，美國企業對於員工網路使用與電子郵件內容監看的情形，已經成爲普遍存在的現象。例如根據 AMA 所作的調查顯示，已經有高達 78%的美國雇主表示對員工的網路與電子郵件採取某種形式的監看，其中更有 63%的雇主監看員工網路使用情形，47%的雇主會儲存並審閱員工的電子郵件[156]。而在另外一份由過濾軟體公司 SurfControl 所進行的調查也得到類似的結果。該研究發現在 2001 年有超過 75%的企業表示，必須使用過濾軟體或是其他監控技術，以防止員工在上班期間爲私人目的而使用網路。

電子郵件監看問題的產生，在於雇主與員工對電子郵件的性質認知不同。就雇主的角度而言，員工使用公司的電腦設備，本應該執行公司的業務，否則即是一種資源的浪費，因此，雇主應有權對員工執行職務的品質加以監控。但在員工的立場而言，員工會認爲他們的電子郵件內容是個人的隱私，至少是一種隱私的期待，雇主任意監看他們的電子郵件，當然構成通訊隱私權之侵害。因此，企業內雇主是否可以有權利利用電子監看系統來監視員工的電子郵件，並檢查其所使用的電子郵件，乃是一件極爲爭議的法律問題。我國司法實務亦受美國法影響。故

---

http://www.ntia.doc.gov/reports/anol/NationOnlineBroadband04.htm（最後瀏覽日期：2007 年 11 月 11 日）

[154] Jay P. Kesan，*Cyber-Working OR Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*，54 FLA. L. REV. 289,290（2002）

[155] 請參見 Employers Read Workers' Email, http://www.wired.com/news/business/story/19152.html. 轉引自馮震宇，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，月旦法學第 85 期（2002 年 6 月），頁 89。

[156] 請參見 Eric J. Sinrod., Electronic surveillance in the workplace, Oct. 18, 2001, http://www.usatoday.com/life/cyber/ccarch/2001/10/18/sinrod.htm. 轉引自馮震宇，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，月旦法學第 85 期，頁 89。

本章將探討美國對此問題之立法例及實務見解，以瞭解本問題爭議所在。

第二節　美國關於企業是否可監控員工電子郵件的爭議

一、美國有關隱私權保護規範

美國憲法中對隱私權並無明文規定，而在 Griswold v. Connecticut[157]以及 Roe v. Wade[158]等案件中，聯邦最高法院認爲隱私權概念仍在美國憲法第 1、第 4、第 5 增補條款中有跡可循，而第 5 及第 14 增補條款更可作爲隱私權的法源基礎。但這裡所指隱私權，偏向基本權利（fundamental rights）類型的活動，即關於婚姻、生育、避孕、家庭關係、對子女的養育與教育等性質活動。在實踐上，個人資訊隱私權常常是以間接的方式受到保護－亦即如果不保護個人隱私的話，個人其他憲法上權利將會受到侵害。例如在 ***NAACP V.Alabama***[159]一案中，最高法院之所以禁止政府機構取得「全國有色人種權益促進會」（NAACP）的會員名單，是因爲 Alabama 州政府的行爲反了憲法第 1 增補條款的結社自由，而這樣的決定也間接保障了 NAACP 會員的隱私權[160]。

就聯邦立法而言，爲防止政府對於人民隱私權侵害，或者就各個特定隱私權領域而分別加以立法。例如 1968 年的聯邦竊聽法（Federal Wiretap Act[161]）、1974 年的隱私權法（The privacy Act[162]）、1974 年的家庭教育權利及隱私法（The Family

---

157 381 U.S.479（1965）。

158 410 U.S.113（1973）。本件聯邦最高法院指出，隱私權不僅只個人資訊的控制，亦包括個人發展上之自主決定。

159 357 U.S.449（1958）。

160 王郁琦，工作場合中電子郵件隱私權之研究，收於氏著「資訊、電信與法律」，元照出版，2004 年 5 月，頁 93-94。

161 1968 年的聯邦竊聽法係爲了保護人民透過線路傳遞聲音的隱私權（即電話的隱私權）。

162 1974 年的隱私權法乃資訊自由法（The Freedom of Information Act）的姐妹法。旨在妥善規範

Education Rights and Privacy [163])、1978 年的財務隱私權法（Rights to Financial Privacy Act[164])、1986 年的電子通訊隱私權法（Electronic Communication Privacy Act，ECPA[165])、1994 年的法律執行通訊協助法（Communication Assistance for Law Enforcement Act[166])。

但工作場所隱私的保護，在美國長久以來相對受到忽視。有學者指出，這是因爲過度強調僱用自由意志原則（employment-at-will）的結果。且依美國現行法制，限制員工於工作場所隱私，只要經雇主預先通知，員工即很難主張隱私的合理期待[167]。

政府使用、交換以及傳遞個人資料，使大部分個人均得向聯邦政府取得其個人資料，確保聯邦政府侵犯個人隱私權，或依不適當之資料做出對個人不公平之決定，促使政府機關對其蒐集或保有之個人資料負起全責。

[163] 由於學校等教育機構，儲存大量涉及學生及其家庭高度隱私的資料，例如學生成績、健康狀況、家庭概況等資料，故爲充分保障學生及父母之隱私權，美國 1974 年始有家庭教育權利及隱私法（The Family Education Rights and Privacy）的立法。規定未滿 18 歲學生父母及滿 18 歲之學生，有權查詢、請求更正學生之教育資料，學校如任意拒絕，聯邦政府得斷絕經費補費，而學校等教育機構，原則上，未經學生父母同意，不得以知之權利爲由，任意提供學生資料給第三人。

[164] 1978 年的財務隱私權法（Rights to Financial Privacy Act）乃爲限制聯邦政府自私人金融機關取得個人的財務資料，而課以金融機關保持秘密的義務。

[165] ECPA 制定目的是爲了補充 1968 年的聯邦竊聽法（Federal Wiretap Act） 的漏洞。制定背景是因 1960 年代的水門事件（Watergate）醜聞案後，爲反制政府不當竊聽電話而制定。 ECPA 主要係針對網路監聽（聲音訊息）以及電子郵件（非聲音訊息）之隱私權保護。此外，該法也擴充禁止非法監聽對象及於個人，而不再單及於政府的非法竊聽。

[166] 1994 年的法律執行通訊協助法（Communication Assistance for Law Enforcement Act），主要立法目的係藉由提供經費幫助包括 AT&T，Ericsson 等電話公司使其設備升級，以配合法院監聽命令。雖然法律執行通訊法協助提供了竊聽傳統電話的合法依據，但對於網路電話（Internet-Phone）是否亦可以加以合法竊聽則仍有爭議。此乃因傳統電話是點對點、一對一的對話，若進行竊聽原則上與受監聽者以外之他人無關；但就網路電話而言，由於網路上資料的傳輸是透過封包（Package）交換的方式來完成，若執法者進行網路電話監聽時，即有可能同時侵害到受監聽者以外之他人的通訊內容，此時即有爭議。請參見資訊法務透析，87 年 12 月號，國際動態，頁 14-15。

[167] Michael Selmi，*Privacy for the Working Class: Public Work and Private Lives*，66 LA. L. REV. 1035，1036（2006）

二、　電子郵件概說

(一) 何謂電子郵件(Electronic Mail; E-Mail)

利用網際網路 (Internet)，做無連接式(Connectionless)的訊息傳送或接收。如一般信件郵遞方式，指明收件者地址 (E-mail Address)，即可透過網路，由一端之電腦傳送訊息至另一端。在許久之前，電子郵件仍然是以大型或迷你級電腦爲發展基礎，只有少數的專業人員在使用。隨著區域網路的普及以及個人電腦深入家庭，電子郵件的使用愈加普遍。連接 Internet 的電子郵件系統可以對所有 Internet 上的用戶收發信件，由此想見電子郵件是全球性且經濟的訊息傳輸方式。發送電子郵件並非難事。只要將內容在電腦上完成，指明收件人的地址(E-Mail Address)，再用簡單的指令，就可在極短的時間內，將內容傳給對方，而收信會自動存放在你的帳號下，隨時等待你開啓電腦來看信。

（二）電子郵件的架構

電子郵件是以無連接式訊息封包(Package)傳送。 以寄信而言，使用者完成信件內容後，下指令寄信，則封包透過電子郵件伺服器(Mail Server)， 根據電子郵件協定 (如 SMTP；MIME) 封裝，然後經網路 (Internet 或 TCP／IP 網路)傳送至收信端的的電子郵件系統。一般而言，你只要在伺服器(Mail Server)上有帳號(login)，電子郵件系統會以這個帳號來當做你的電子郵件地址(E-Mail Address)[168]。在所有的電子郵件信箱中，都有一個 「@」符號。在「@」符號左邊所列者爲 Local 名稱，即使用者名稱。在「@」符號右邊所列的，則爲 Domain 名稱，即使用者所屬之網域名稱。電子郵件可分爲內容與地址兩個部分[169]。本文係針對內容部分討論。

---

[168] http://www.nhlue.edu.tw/ccenter/Page/mail.htm#mailer（最後瀏覽日期：2007 年 11 月 11 日）

[169] 電子郵件的內容享有較嚴謹的保護；電子郵件地址部分，依 Smith v.Marylan 案（442 U.S.735（1979））判決，當事人所撥電話號碼無法主張隱私的合理期待。而在 United States v.Hambrick 案中，法院認爲 Kaze 案之合理隱私期待僅適用於電子郵件內容，而不適用於電子郵件地址。

（三）企業內部網路（intranet）

電子郵件便利、速度、成本效益及可大量存取的特點，已使得電子郵件及網際網路成爲現代商業不可缺少的部分工具。一項調查顯示，在 90 年代初期，電子郵件使用佔美國全部大公司的百分之七十五。晚近的研究發現，每年透過電子郵件聯絡溝通的雇員數量預估將以每年的百分之二十的比率成長。歐美各大企業目前都有專責部門來處理電子郵件的對外窗口，從商務往來、招募新手、解決糾紛到內部改良，不但時效驚人，效果也相當好。對於電子郵件「冷感或操作不良」的企業，幾乎已經被摒棄在「現代科技」的大門外，更別說是企業形象或是業績提升了。

許多知名大企業也紛紛建置內部網際網路（intranet）。

Intranet 係以 Internet 之技術標準爲基礎，兩者共通點在於：使用相同之軟體、網路設備與通訊協定與標準。易言之，兩者都是採 TCP/IP 通訊協定、以 HTML 作爲文件交換標準、以瀏覽器（ Browser）爲使用者之界面、支援跨機器平台之開放系統。

企業內部運用時，其意義與重要性在於[170]：

1.透過文件管理系統，將企業內部之各種資料文件予以有效整合、管理，而所有員工都能透過 Intranet，使用瀏覽器迅速在其權限內取得所需資訊。

2.企業內部流程之再造：在 Intranet 運作上，不僅文件之發送與管理電子化，企業內各項工作、業務與管理之流程也全部電子化，並透過電腦管理系統加以管理。使企業內部運作更有效率。特別是可以透過 Intranet 來管理分散各地之各式伺服器，或將重要資源集中管理。

3.有助於企業內部資訊文化的形成：不僅企業內各項作業流程均透過 Intranet 進行，Intranet 亦可作爲企業內部連絡管道，可增加員工間及員工與管理者間之互動溝通與討論。

[170] 謝銘洋，企業內部網路（Intranet）法律問題，萬國法律 47 期（1999.4），頁 42。

4.有助於提升企業競爭力。

但對於安全控管問題，在防止他人入侵部分，多依賴防火牆。但內部的安全管理，特別是電子郵件，因員工透過電子郵件彈指間即可將各種企業內部資料傳送出去，企業擔心資料安全，有些完全禁止員工使用電子郵件對外聯絡；有些企業要求員工對外傳遞的電子郵件必須經專業人員檢查後才能寄送。有些企業並不要求所有電子郵件必須經檢查後才能寄送，亦不於事後全面檢查，而是對員工所有對外往來之電子郵件都存檔備查，嗣後再爲抽查或針對有問題員工之信件加以檢查。

三、雇主監看員工電子郵件的正當化理由與監看形式

（一）監看理由

雇主監看員工電子郵件的正當化理由不外基於下列幾點理由[171]：

1.基於工作效率：避免系統因員工個人使用而擁塞當機、避免商業機密外洩。 監控員工在工作場所的生產力[172]、使電腦使用最大化。

2.監控員工是否遵守雇主關於工作場所使用電腦系統、電子郵件系統和網際網路有關的政策。

3.調查員工不端行爲， 包括性騷擾和歧視的申訴。

4.防止智慧財產權損失：營業秘密被認爲是公司最有價值的資產。營業秘密 的定義包含，任何程式、圖形、編輯、計畫、設備、方法、技術或者製程等有獨立的經濟價值者[173]。因此，防止或者發現工業間諜行爲，例如竊取商業機密和內部

---

[171] Gail Lasprogata, Nancy J. King, Sukanya Pillay，*Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 4（2004）

[172] Paul E. Hash & Christina M. Ibrahim, *E-Mail, Electronic Monitoring, and Employee Privacy*, 37 S. TEX. L. REV. 893, 897 (1996).

[173] Unif. Trade Secrets Act 1(4) (2004).

訊息，侵犯著作權、專利權或者商標的行爲[174]，也是雇主監控的主要理由。

5.爲了防止電腦駭客的入侵[175]。

6.保護電腦，以防超載。

7.爲了防止或者發現犯罪活動和恐怖主義活動[176]。

8.回應有關訴訟中對電子證據的請求。

9.減少敵意工作環境之訴訟：此乃基於就業歧視與性騷擾等法律責任的避免。雇主提供電腦系統可能因爲員工寄發關於性騷擾、種族歧視、毀謗、侵害著作權等電子郵件而招致損害賠償訴訟。電子郵件笑話、不入流的螢幕保護程式或者色情圖片的下載，都可能爲雇主招來性騷擾訴訟。紐澤西州最高法院在 Blakey v. Continental Airlines Inc.案指出，使用雇主提供的電腦系統傳送損毀名譽的郵件造成「敵意的工作環境」（hostile work environment），可依反歧視法（anti-discrimination laws）提起訴訟。理由是，該電子郵件系統（電子佈告欄）是工作場所的延伸，而雇主有責任防止工作場所騷擾事件的發生[177]。換言之，雇主如無法提出已採取合理措施來事先防範或知悉後採取有效方法來阻止等免責抗辯（Affirmative defence[178]），即應負擔損害賠償責任。此外，由於美國聯邦民事訴訟程序規則

---

174 Mike Consol, *Industrial Espionage, The Secret Agents of Fortune*, BUS. J. (1998), *at* http://www.secure-data.com/art9.html（最後瀏覽日期：2007 年 11 月 11 日）

175 Institute for Security Technology Studies at Dartmouth College, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks, A National Needs Assessment*(2002), *at* http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf（最後瀏覽日期：2007 年 11 月 11 日）

176 Michael R. Anderson, *Identifying Internet Activity, Computer Forensics Goes to Cyber Space, at* http://www.forensics-intl.com/artipfl.html
and *Net Threat Analyzer, at* http://www.forensics-intl.com/nta.html（最後瀏覽日期：2007 年 11 月 11 日）

177 Meir S.Hornung , *Think before you type: a look at email privacy in the workplace*,11 FORDHAM J.CORP.&FIN.L.121-123（2005）

178 根據美國最高法院在 Faragherv. v. City of Boca Raton 案之見解，對擁有管理監督權能受雇者 (supervisory employees) 觸犯敵意工作環境性騷擾時雇主之法律責任歸屬，在決定雇主是否符合此一免責抗辯要件時，他 (或她) 應主動提示一「經證明有效之申訴及解決性騷擾控訴機制 (mechanism)，且能供受雇者在不會造成不當危險及花費之情形下加以運用始可。」同時，如果受雇者本身未能運用該項補償性措施 (remedial apparatus) 時，則雇主即不應負擔法律責任。爲更明確表達此一意旨，該院做出下列之判決：「在具有直接 (或更高階層) 權能之管理監督者造成之一可提起訴訟控訴之敵意工作環境時，雇主對被害之受雇者即應負代理法律責任，在這種情形下，若管理監督者並未採取任何涉及有形就業利益之聘僱行爲 (tangible

（Federal Rules of Civil Procedures ）明確的規定，電子郵件不但可在發現或搜查程序中被請求提出，並且在經過適當程序證明該電子文件的真正原始身份後，亦可在訴訟程序中被提出來作爲證據。因此在許多訴訟案件中，員工的電子郵件往往被作爲攻擊雇主的主要攻擊、防禦手段之一，如此一來，使得企業紛紛選擇對員工電子郵件加以監看。

（二）監看形式

監看的形式，可能透過監控軟體系統，使雇主得以秘密、即時監控員工電腦網路的連線，這些系統能有的可由關鍵字和片語掃描電子郵件。藉由監控軟體，可顯示受僱人的線上活動，包括聊天室、程式、線上遊戲、檔案使用及下載、下載所花費時間及收發電子郵件。此外，監控軟體也可監控員工電腦硬碟以辨別色情圖片或違反著作權法下載的音樂、電影。即使是非以監控爲核心目的的軟體，例如，反毒和垃圾郵件軟體，可以被使用來監控。有些系統可能記錄每次電腦鍵盤敲擊鍵，測出每分鐘的擊鍵速度、完成工作所花費及休息的時間，而不被員工察覺。有些軟體尚可追蹤電子郵件[179]。這些系統經常未經通知員工的情形下即安裝[180]。

---

employment action)，則雇主即可根據聯邦民事訴訟法第八 (c) 條之規定，以一項具優勢之證據 (a preponderance of the evidence)，來對法律責任或損害賠償金之訴 求提出一項免責抗辯。此一免責抗辯應包含兩項必要條件： (a) 雇主已採取合理之注意，來避免及迅速糾正任何性騷擾行爲；及 (b) 原告受雇者在不合理之情況下，未能充分利用雇主所提供之預防或糾正措施，或未能避免此類傷害之發生。」。此外，爲避免此一判決還有任何含混不清之處，該院多數意見更進一步指出：「在雇主提出第一項免責抗辯之訴訟時，他 (或她) 是否曾頒布一項包含申訴程序之禁止性騷擾政策聲明一事，雖非在任何情況均屬法律上所必要者，然而，至少要備有一適合 (事業單位) 就業情況之正式政策聲明，則仍屬得以合宜探討之處。同時，就受雇者未能採取合理注意之相對義務方面而言，也並不僅侷限於她 (或他) 未能合理運用雇主所提供之申訴程序此一情形而已，雖然前述之舉即足以充分符合雇主第二項免責抗辯之必要條件。」請參考，焦興鎧，美國最高法院與工作場所性騷擾之爭議，歐美研究第 32 卷第 2 期（90 年 6 月），頁 357-363。

[179]例如，在喧騰一時的惠普公司監聽醜聞案，惠普公司(Hewlett-Packard)一名調查人員表示，該公司在送給 CNET News.com 記者的檔案中，使用一個商用服務，可以追蹤電子郵件的傳送路徑。在美國國會眾議院聽証會上作証時，惠普的安全主管 Fred Adler 表示，HP 的調查員使用 ReadNotify.com 公司的服務，來追蹤一封送給記者 Dawn Kawamoto 的電子郵件，以試圖得知她新聞消息的來源。 在 HP 的董事會紛爭事件爆發之後，Adler 的作証首度確認該公司追蹤傳送給 awamoto 電子郵件的方法。同時 Adler 還表示在一些特定的情況下，使用電子郵件監控技術是公司的慣例。由 ReadNotify 服務的特性來看，使用的似乎是所謂的網路機器人技術，這個技術也常被一些電子郵件廠商使用。只要透過 ReadNotify 技術傳送的電子郵件或是文件，都含有該服務所嵌入的一或多個隱藏的檔案連結。當郵件訊息或檔案被開啓時，郵件程式會接收檔

第三節　美國關於企業電子郵件監看的立法例

一、美國關於工作場所隱私的保護----公/私領域的區分

在美國，工作場所隱私保障因循公領域（public sector）、私領域（private sector）的劃分。也就是說，員工在工作場所隱私保護的範圍與依據，端視他們爲政府部門工作或者在私營企業工作而有不同。憲法權利主要保護公民以對抗政府行爲，政府機關員工可能據此主張憲法的權利，反之，私營企業員工則無法據以主張。舉例來說，關於工作場所搜索和監督行爲，政府部門員工可能主張憲法增補條款第 4 條所保障的，禁止不合理的搜索扣押。而私營企業員工基本上只受到普通法、州法和聯邦法保護。

二、公部門員工的保障---憲法增補條款第 4 條[181]的保護

（一）O'Connor v. Ortega[182]案揭示的原則

案例事實：

案，這時便會通知 ReadNotify。 一般來說收件者並不會意識到這個連線動作。電子郵件是由 HTML（超文字標記語言）所構成，因此內含的追蹤檔案並不會顯示。接收檔案的實際連結只有在觀看電子郵件的原始碼，比方使用記事本之類的文字程式時，才會顯示出來。然而如果有裝設防火牆，則還是會警告使用者網路連線的出現。參考，http://taiwan.cnet.com/enterprise/technology/0,2000062852,20110604,00.htm（最後瀏覽日期：2007 年 11 月 11 日）

[180] Todd M. Wesche，*Reading Your Every Keystroke: Protecting Employee E-mail Privacy*，1 J. HIGH TECH. L. 106,107（2002）.

[181] "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."

[182] O'Connor v. Ortega, 480 U.S. 709 (1987).

本案加州州立醫院精神科醫師 Ortega 因涉嫌強迫住院醫師爲其購買蘋果牌電腦、對一位醫學院學生做出不適當處分、以及性騷擾兩名員工等情形遭調查。於 Ortega 休假期間，醫院執行長 O'Connor 選擇幾所醫院進行調查。相關調查人員多次進出 Ortega 醫師的辦公室，並扣押了一些醫院辦公室中的物品（包含 Ortega 的私人物品），並未與 Ortega 的個人財產作區分[183]—實際上，Ortega 的財產與州立醫院的財產一起裝箱[184]，且沒有製作扣押清冊[185]。

Ortega 遭解僱後，以 O'Connor 醫師及醫院相關調查人員違法搜索他的書桌和檔案櫃，侵犯他憲法第 4、第 14 增補條款所保障的權利爲由，提起損害賠償訴訟。地方法院駁回原告之訴，判決醫院勝訴，認爲了保全州政府的財產所爲搜索是正確的[186]。但經 Ortega 提起上訴後，聯邦第九巡迴法院廢棄原判決，並發回更審[187]。醫院因此上訴聯邦最高法院。

判決結果：

本案美國聯邦最高法院最後以五比四的票數，判決認定本案構成憲法增補條款第 4 條的違反。

解釋方法與確立的原則：

O'Connor v. Ortega 案的解釋框架由憲法增補條款第 4 條開始，該條保證人民有保護其身體、住所、文件與財物，不受不合理搜索和扣押的權利。憲法增補條款第 4 條建立於「正當隱私期待」（legitimate expectation of privacy）[188]的存在。要確定是否有隱私的正當期待存在，須具備兩個要件：

---

[183] *Id.* at 713-14.

[184] Court records indicate that the investigators did not separate Dr. Ortega's property from state property. Indeed, one investigator testified, "trying to sort State from non-State, it was too much to do, so I gave up and boxed it up." Id.

[185] "All the papers in Dr. Ortega's office were merely placed in boxes, and put in storage for Dr. Ortega to retrieve." Id. at 714.

[186] O'Connor, 480 U.S. at 714.

[187] O'Connor, 480 U.S. at 714.

[188] Rakas v. Illinois, 439 U.S. 128, 143 (1978).

（1）隱私的主觀期待表現在搜索範圍中。（2）該隱私的期待社會普遍認爲是合理的[189]。

O'Connor v. Ortega 案，美國最高法院討論了第 4 增補條款的適用範圍後，肯定員工就個人辦公室、辦公桌、檔案櫃可能有隱私的合理期待存在。但這樣的合理期待仍需衡量政府因監督、控制和有效率工作場所的需要[190]。

多數意見說明政府雇主對於員工工作場所的搜索應受到憲法的評價。首先，法院必須個案認定員工是否有合理的隱私期待。本案 Ortega 獨自占有該辦公室十七年；此外，醫院亦無任何規章或政策禁止個人於檔案櫃置放個人物品。應有隱私的主觀期待。如果認爲有隱私的合理期待，接下來要問的，就是搜索扣押是否合理。法院的結論認爲，要求雇主欲進入員工的辦公室，書桌，或檔案櫃爲與工作有關的目的必須取得令狀，將嚴重擾亂例行業務管理活動，並不合理。 此外，要求搜索有相當理由（probable cause），會對政府雇主施加無法容忍的負擔。根據多數意見的見解，對於政府員工憲法保護的隱私利益應依相關情況判斷「相當」的合理性。另外，多數意見也指出，搜索的範圍必須合理。

（二） *O'Connor v. Ortega* 案的原則適用於電子郵件？

關於電子郵件監看的問題， *O'Connor v. Ortega* 案無疑提供將政府機關受僱員工於電腦及其中內容有固有隱私權和和財產權與憲法增補條款第 4 條並列的基礎。在 *O'Connor v. Ortega* 案，政府部門的員工在他們的工作上享有充分的隱私期待。電腦資料最初被創造時，有類似的隱私期待存在。如果該儲存的資料只授權給選定的使用者接觸（access），隱私的合理期待將得到更進一步支持。要決定是否有合理的隱私期待存在，須視具體的情況而定。電腦密碼是決定是否有隱私

189 U.S. v. Anderson, 154 F.3d 1225, 1229 (10th Cir. 1998)

190 “what is a reasonable search depends on the context within which the search takes place, and requires balancing the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace”. O'Connor, 480 U.S.at 719-20

期待存在的重要關鍵點。在 *U.S. v. Slanina*[191]案，法院認爲，行政機關授權給員工密碼和鑰匙進入電腦和辦公室，這些行爲就是主觀隱私期待的證據。再者，當雇主未通知員工電腦可能被監控，而員工可進入其他人的電腦時，主觀的期待可能提升到社會普遍認爲是合理的客觀標準[192]。對政府機關員工來說，關於電子郵件案件，第 4 增補條款已經成爲保護隱私的有效方法。但仍必須具備「合理的隱私期待」（reasonable expectation of privacy）。合理期待的隱私須具備兩種要素：實際(主觀)隱私期待（actual (subjective) expectation of privacy）和社會普遍認爲是合理的（the expectation be one that society is prepared to recognize as reasonable）。

法院已經將憲法增補條款第 4 條運用至對政府員工所爲的電子監視[193]。事實上，至少有一個法院認爲，政府雇主在工作場所爲電子監控並未符合工作場所搜索須具備「合理性」（reasonableness）的合憲要求。

理由是對活動和談話的電子監控比實際的人爲搜索侵犯的隱私利益嚴重[194]。此

---

191 U.S. v. Slanina, 283 F.3d 670, 676 (5th Cir. 2002).

192 Lee Nolan Jacobs, *Is What's Yours Really Mine?: Shmueli v. Corcoran Group and Penumbral Property Rights,* 14 J.L. & Pol'y 837,867（2006）

193 See, e.g., Lukas v. Triborough Bridge & Tunnel Auth., No. CV-92-3680 (CPS), 1993 WL 597132, at *5-*7 (E.D.N.Y. Aug. 18, 1993) (holding that employees have reasonable expectation of privacy against having their conversations monitored in workplace, even when that workplace is tollbooth); United States v. Maxwell, 42 M.J. 568, 575 (C.A.A.F. 1995) (recognizing that individual can have objectively reasonable expectation of privacy in electronic mail messages transmitted on on-line computer service while those messages were stored on service's computers). The Maxwell court's reasoning further suggests that public-sector employees would also have objectively reasonable expectations of privacy that their electronic mail messages will not be routinely accessed. According to the court, [A]ppellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that appellant's computer transmissions would be received by anyone other than the intended recipients. Maxwell, 42 M.J. at 576. But see David E. Steinberg, Making Sense of Sense-Enhanced Searches, 74 Minn. L. Rev. 563, 583-88 (discussing "cultural criticism" of Fourth Amendment jurisprudence which places primary emphasis on physical trespasses in determining reasonable expectations of privacy).

194 See Varnado v. Department of Employment and Training, 687 So. 2d 1013, 1024-30 (La. Ct. App. 1996) (holding that state employer illegally read and copied employee's computer files because employee had reasonable expectation of privacy in his computer and its files, and employer had no justification for search). But see Williams v. Philadelphia Hous. Auth., 826 F. Supp. 952, 954 (E.D. Pa. 1993) (holding that municipal employee had not stated Fourth Amendment violation when his employer reviewed diskette, containing work and personal material, that he had left on his desk); Star Publ'g Co. v. Pima County Attorney's Office, 891 P.2d 899, 901 (Ariz. Ct. App. 1994) (doubting that "public employees have any legitimate expectation of privacy in personal documents that they have chosen to lodge in public computer files").

外，法院認定，對政府員工實施錄影監視的是「異常侵入方法的搜索」（extraordinarily intrusive method of searching[195]）。

然而憲法增補條款第 4 條提供的保護未必皆適用於電子郵件的情形，以下舉幾則相關案例：

1. United States v. Maxwell

本案是關於工作場所電子郵件搜索的一個重要判決。本案電子郵件是透過私人線上服務系統--美國線上（America On-Line， AOL[196]）提供。本案當事人 James A. Maxwell,是美國線上的用戶，有 4 個專用的線上認證帳號（Screen Name）或身分[197]。FBI 得到情報：Maxwell 使用他美國線上的電子郵件帳號傳送兒童色情圖片。FBI 於是申請搜索令搜索可疑的美國線上的 9 個用戶的電子郵件通訊（包含 Maxwell 的線上認證帳號）。

空軍刑事上訴法院（The Air Force Criminal Court of Appeals）認爲本案構成憲法增補條款第 4 條保護的搜索[198]。

Maxwell 有客觀合理的隱私期待—因爲那些儲存在電腦裡的訊息資料只有使用他自己的密碼才能讀取。同樣地，被告對於傳送給其他美國線上用戶的電子郵件也有隱私的客觀期待，因爲其他用戶也分別有指定的密碼[199]。

---

[195] State v. Bonnell, 856 P.2d 1265, 1273 n.5 (Haw. 1993). The Bonnell court held that intrusive video surveillance violated postal employees' reasonable expectation of privacy in their break room; see also Vega-Rodriquez v. Puerto Rico Tel. Co., 110 F.3d 174, 180 n.5, 184 (1st Cir. 1997) (upholding videotaping of public work area, but cautioning that cases involving covert use of clandestine cameras or electronically- assisted eavesdropping require different analysis); United States v. Taketa, 923 F.2d 665, 675-76 (9th Cir. 1991) (finding that video surveillance is Fourth Amendment search requiring warrant and noting its intrusive character (citing United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987).*See* S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in The Workplace*，32 GA. L. REV. 825,873（1998）

[196] AOL 爲提供全球線上服務的網際網路服務提供者（ISP）。

[197] AOL 要使用者註冊 Screen Name 才能使用網路化存取服務 My AOL、電子郵件及行事曆等。AOL 允許一個帳戶可以有七個線上認證帳號（Screen Name）--1 個主要線上認證帳號和 6 個其他名稱；主要線上認證帳號是永久;無法改變，但其它 6 個得隨時創設或刪除。參考，http://www.dummies.com/WileyCDA/DummiesArticle/id-1335.html

[198] United States v. Maxwell, 42 M.J. 568 (A.F. Ct. Crim. App. 1995).

[199] See Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation of Privacy*, 8 J. Tech. L. & Pol'y 135,147-149.（2003）

1996 年 6 月，本案經上訴法院（the Court of Appeals for the Armed Forces）審理後，同意原審的結論，但是增加幾個具有指標性的觀點[200]。首先，法院認爲以電子郵件溝通與電話交談相似，因此，如果有合理的隱私期待存在，應受到憲法增補條款第 4 條的保護。其次，就被告與美國線上之間契約約定而言，美國線上有確保 Maxwell 隱私的契約義務。 最後，上訴法院認爲，在被告和其他美國線上用戶間的電子郵件談話內容有合理的隱私期待。

另外，上訴法院也注意到美國線上提供比其它類似網際網路上的電子郵件系統更多的隱私，因爲這些儲存在公司私人擁有的電腦資料庫的訊息，不會被讀取或對任何人揭露--包括美國線上的執行者。美國線上用戶不僅對他們的電子郵件訊息有隱私的合理期待，而且包括儲存在在美國線上的電腦上的那些訊息。 它也伴隨產生警察不僅於即時監視電子郵件通訊需要取得搜索令，要搜索網路儲存於網際網路服務提供者的舊檔案也必須取得搜索令。

總括而言，*Maxwell* 法院認爲，在現代通訊時代，社會承認電子郵件有合理隱私期待。依據法院觀點，電子郵件的電子通訊本質不是對其提供隱私保護的障礙[201]。只是須受客觀合理隱私期待的檢測。

2. Bohach v. City of Reno[202]

本案是另一件與接觸儲存在電腦上的電子訊息有關，涉及憲法增補條款第 4 條的案例。

本案與 *Maxwell* 案涉及私人業者提供的電子通訊不同，本案涉及的是政府運作的電腦系統--電腦化的傳呼系統（The computerized paging system,Alphapage）。該系統由雷諾市警察廳提供，允許用戶製作發送簡短文字或者聲音訊息透過區域網路系統傳呼接收者。

---

200 United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).

201 Rebecca Ebert,Mailer *Daemon: Unable to Deliver Message Judicial Confusion in the Domain of E-Mail Monitoring in the Private Workplace*，1 J. HIGH TECH. L.67-69（2002）

202 Bohach v. City of Reno,932 F. Supp. 1232 (D. Nevada 1996).

警政廳的兩名警員，Bohach 和 Catalano，因傳送到彼此傳呼器的通訊內容受到內部調查，主張憲法上隱私的權利受到侵害。

地區法院同意他們有主觀的隱私期待，否則他們不會發送引發調查的訊息。不過，法院判決結論基於下列理由認爲沒有客觀的合理期待：

首先，法院認爲，本案並未攔截或竊聽有線通訊，該發送的訊息是基於電腦系統運作產生的儲存訊息。其次，法院認爲，系統實際上爲任何人所易接近，而且使用時並沒有特別的密碼。第三，系統的主要目的係與工作相關的業務聯繫，而非私人通訊。第四，事實上，某些類型的訊息，例如該系統禁止對部門政策的評論，用戶擁有較少的隱私期待。最後，電腦的服務提供者，也就是雷諾市，依該市法令可以接觸電子儲存的通訊。

Bohach 法院認爲本案當事人透過區域網路系統（LAN computer system）交換的訊息沒有隱私的合理期待。導致本案與 *Maxwell* 案有不同結論在於有幾個主要不同的區別。在 *Maxwell* 案，Maxwell 以個人費用購買所有的電腦硬體、 軟體，和申請網際網路系統帳號，而本案原告使用警政廳的電腦終端機（terminal）、電腦（computers）、軟體（software）和傳呼機（pagers）。 另一個重要區別，是系統原先預設的用途本質不同。美國線上與公務不相關且不以監控爲目的，而傳呼機（Alphapage）的安裝，係爲簡化警察工作，並且考慮到警察人員之間資料的即時交換，因此，隱含有監控目的。

Bohach 法院甚至認爲，本案訊息的傳輸是透過部門的電腦系統，因此，即便是攔截通訊，結論也無不同。

3. Haynes v. Office of the Attorney General[203]

在 *Haynes v. Office of the Attorney General* 案，一名前堪薩斯州法務部助理 Carlus Haynes，請求核發禁止令（injunctive relief），以阻止他的前雇主接觸他工作電腦

[203] Haynes v. Attorney General of Kansas, 2005 WL 2704956 (D. Kan. Aug. 26, 2005)

的私人檔案。

本案事實圍繞著 Haynes 被解僱以及隨後禁止電腦資料的存取。

原告 Haynes 被告知他的電腦有兩個檔案夾—私人用和公共用（private and public），他可以將私人訊息儲存在私人檔案夾，沒有人會接觸這些資料。

堪薩斯州法務部訂有電腦使用的政策，當員工一打開電腦就可看到顯示的政策規定[204]，部分內容如下：

「辦公室電腦的使用應符合使用程序…。 …電腦作爲非公務授權使用僅允許於最低限度的時間和頻率且不干預州政府目的下。本系統不得用於非法或其他使使用者、收件者或法務部難堪的目的。…使用本系統沒有隱私的期待，但禁止未經允許故意接近其他使用者的電子郵件，除非經授權使用電腦的程序。 … 儘管將檔案刪除，檔案可能仍可儲存於電腦備份檔，個人儲存於電腦上的資料可能被移除。… 」

除此以外，原告從未由他的雇主處收到任何其他的電腦使用政策或程序的通知。

Haynes 在被通知他將要在兩週後被解僱的同一天，他的監督主管與一位電腦專家聯繫，限制 Haynes 的對電腦的存取權限，並保證沒有資料被複製。當 Haynes 存取他的電腦並且開始複製他的個人檔案和工作上的產物時，他的主管接觸他的資料並且指控他偷竊。Haynes 解釋他正複製他的個人檔案。大約 1 小時後，Haynes

---

[204] Haynes v. Attorney General of Kansas, 2005 WL 2704956, 2 (D. Kan. Aug. 26, 2005). The full policy read as follows:
Office computer use shall be in compliance with computer use procedures. Obtain full procedures from your deputy or supervisor. Computer use for non-official business is authorized only if kept to minimum duration & frequency & if it does not interfere with state business. This system shall not be used unlawfully nor for any purpose which could embarrass the user, recipient or Attorney General. There shall be no expectation of privacy in using this system; however, intentional access to another user's e-mail without permission shall be prohibited, except as authorized by computer use procedures. Despite deletion, files may remain available in storage. Personal data on the system may be subject to removal. Data may be subject to state public records and records preservation laws. User software installation is prohibited unless specifically authorized. Software may not be copied for use outside this office unless authorized.

被立即解僱，並限他 15 分鐘內離開，而且沒讓他帶任何東西，包括個人物品。在他被解僱之後，他的電腦上的檔案，包括個人電子郵件訊息，被其他員工閱覽。原告主張憲法增補條款第 4 條、第 14 條之權利受侵害。

Haynes 法院援引 *O'Connor* 案的框架確定是否有正當的隱私期待 存在。當 Haynes 受僱時，他在辦公室電腦上電子郵件使用說明簽字同意。每次 Haynes 登入到他的電腦就可見到明確警語，事前告知他（及全部員工），電腦的使用沒有隱私的期待，個人儲存於電腦網路上的檔案，隨時可能未經通知即被移除。

該警語成爲法院決定否准禁止令的要素。最後，法院認爲 Haynes 未能證明有客觀的合理隱私期待。不過，法院也注意到關於隱私的期待的法律狀態，有嚴重視每一個案特別事實而定的情況[205]。

（三）評論

1. 法律 vs 科技

正如同 Clark 大法官的感嘆：「法律雖然小心守護個人隱私，但並未跟上科技方面的發展。[206]」

Harlan 大法官於 *Katz* 案明白解釋了美國憲法增補條款第 4 條保護的是人（people），而不是場所（places）。推翻了原先物理空間非法侵入（trespass or"physical penetrations"）的認定標準[207]，將憲法增補條款第 4 條的搜索的範圍擴大至物理空間以外的非法侵入[208]。

---

205 Lee Nolan Jacobs, *Is What's Yours Really Mine?: Shmueli v. Corcoran Group and Penumbral Property Rights,*, 14 J.L. & Pol'y 837,868（2006）

206 "the law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge",*See* Berger v. New York, 388 U.S. 41, 49 (1967).

207 Katz overruled an earlier case, Olmstead v. United States, 277 U.S. 438 (1928), in which the Court held that a physical penetration or trespass was necessary in order to invoke the Fourth Amendment. see also Katz, 389 U.S. at 353 ("We conclude that the underpinnings of Olmstead ... can no longer be regarded as controlling.").

208 Katz, 389 U.S. at 353 (Harlan, J., concurring) ("Once it is recognized that the Fourth Amendment protects people - and not simply 'areas' - against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical

Katz 案除了指出無令狀的電子監視（electronic surveillance）構成美國憲法增補條款第 4 條規定的不合理搜索外，也建立了隱私期待的標準—法院採取兩部分測試—美國憲法增補條款第 4 條下的合理期待的隱私須具備兩種要素：實際(主觀)隱私期待（actual (subjective) expectation of privacy）和社會普遍認爲是合理的（the expectation be one that society is prepared to recognize as reasonable）。

「社會普遍認爲合理」須檢驗許多事實，例如該訊息是否具有私人性質及個人是否有意公開該訊息（"knowingly exposed" the information to the public）。

自 Katz 案以來，電話通訊已受到憲法增補條款第 4 條的保護--不管是在家裏或在電話亭。

O'Connor v. Ortega 案確立了公部門員工於憲法增補條款第 4 條的保護範圍。

憲法增補條款第 4 條已擴及適用於禁止政府從事某些監控，除非它能夠證明有監控必要。在 ***Chandler v. Miller***[209]案，美國最高法院認爲 Georgia 州法規強制對各政黨候選人進行藥物檢驗，因該州尚未發現有濫用藥物的國家公務員或候選人，也未能證明其依一般執法手段無法充分解決任何潛在的問題，未滿足憲法增補條款第 4 條的「特殊需求」（The Special Needs Doctrine）。

依據 *Chandler* 和 *O'Connor* 案，無任何懷疑即監測個人談話或活動，可能會構成憲法增補條款第 4 條的不合理搜索扣押。

但電子郵件通訊，由上面的案例看來，*Maxwell* 法院承認電子郵件有合理的隱私期待，認爲該案構成憲法增補條款第 4 條的「搜索」。但本案所涉爲刑事案件，爭點在於是否超出搜索的範圍。但由 ***Bohach v. City of Reno*** 及 ***Haynes*** 案看來，對於電子郵件通訊，法院並未給予相同標準的保護。由前開案例所得出結論，政府機關受僱員工透過部門電腦傳輸的訊息，當雇主利用電子郵件使用政策或通知員工時，由憲法增補條款第 4 條提供的保護也相當有限。

---

intrusion into any given enclosure.").

[209] 117 S. Ct. 1295 (1997).

2. 公領域 vs 私領域

公/私區分（the Public/Private Distinction）原先的目的，是要保護個人自由及財產免受政府干預[210]。例如，透過禁止政府干涉個人的政治或宗教信仰、結社等決定權，個人將享有更多的自由和個人自決。

該公/私二分法，也阻止政府通過某些法規和政策增加個人的負擔或限制個人的自由[211]。 二分法意識到，因爲它的權力和範圍，政府應該異於普通公民和私人企業家。

公/私二分法後來也用於區分公有和私人所有權、私營企業（free enterprise）和公共政策（public policy），以及政府雇員和私人雇員。

關於隱私的權利，公/私二分法已將工作場所區分爲公領域與私領域（“public” and “private” sectors）。公部門的勞動關係，包括在地方、州或國家政府部門及其所屬機構。根據定義，它是「政府行爲」 ，並受憲法規範的制約。反之，私領域的勞動關係則常無法適用。諷刺的是，如果不將憲法關於隱私的觀念適用私人雇主，大多數美國雇員幾乎無法保護他們的合理隱私期待。二分法不但沒有強化勞工的自由利益，反而限制他們。因爲私領域不受政府監督或規範的結果，造成私部門雇主得於辦公室、洗手間監視員工，不合理地限制員工的自由和自主。

美國有學者批評指出，當雇主在洗手間裝置監視錄影器，不管公領域、私領域員工，其感受的震驚和憤怒並無二致。事實上，僅公部門員工享有憲法保護的隱私期待，產生的平等對待（即禁止差別待遇）（equal treatment）爭議，亦不容忽視[212]。

---

210 *See* generally Morton J. Horwitz, *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423 (1982) (discussing origins of public/private distinction).

211 *See* Ronald J. Krotoszynski, Jr., *Back to the Briarpatch: An Argument in Favor of Constitutional Meta-Analysis in State Action Determinations*, 94 MICH. L. REV. 302 (1995). at 305-06 (explaining that government cannot necessarily use private companies to execute public policy that has effect of burdening constitutional rights).

212 S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 Ga. L. REV. 825,873-876（1998）

美國學者的批評共識，大多聚焦在該國現行法律架構下，隱私權利於私領域的缺乏，以及於公領域的保障不足，並主張強化員工主觀的合理期待。但亦有反對見解認爲，員工的不端行爲是普遍存在的現實，如果擴大公領域員工的隱私權利，可能增加員工不端行爲，降低政府效率。與私領域有害雇主相較，更有害於社會。而且，如果政府機關被迫移除所有監視設備，將返回由監督者之眼密切監視的時代，反而有害於員工的滿意度和生產力。政府雇主也可能被迫撤除個人可使用的辦公室資源。並且認爲，在公領域，無效率的工作場所也代表無效率的政府[213]。惟本文認爲，不管公領域、私領域工作場所，基於平等權的要求，應受到相同的保護。

三、美國關於企業電子郵件監看之相關立法

就雇主對電子郵件監控，私人企業員工的資源更少，他們通常只有普通法可提供少許的保護。在憲法無法解決的情形下，許多爭議以普通法（Common Law）解決。

（一）普通法及各州侵權行爲法

（1）普通法

在隱私侵權行爲的演化史上，1890 年 Warren 和 Brandeis 教授發表「隱私的權利」（The Right to Privacy）一文等於是宣告隱私侵權行爲法的來臨。其後，William Prosser 教授於 1960 年發表的「隱私」（Privacy）[214]一文，在結論指出，隱私並非一種侵權行爲，而有四種類型：(1)無故侵入私人隱居空間（intrusion upon the seclusion or solitude of another）(2)公開揭露私人事務（public disclosure of

[213] Rachel Sweeney Green, *Privacy in The Government Workplace: Employees' Fourth Amendment and Statutory Rights to Privacy*, 35 CUMB. L. REV. 639,668-669（2004 / 2005）

[214] William L. Prosser, Privacy, 48 Calif. L. Rev. 383 (1960)

embarrassing facts)(3) 誤導(placing another in a" false light" in the public eye) (4)盜用他人的姓名或肖像(appropriation of another's name or likeness)。關於電子郵件監控，員工多主張第一種類型—不合理侵入私人隱居空間(unreasonable intrusion upon the seclusion of another)。主張此種類型的侵權行爲，員工須舉證具備下列三要素：(1) 有意的入侵(an intentional intrusion)(2)高度冒犯(that is highly offensive)(3)員工有隱私的合理期待(the employee had a reasonable expectation of privacy)。「侵入」的要件不限於物理性(physical)，也不須達揭露(disclosure)。

大部分的案件，法院認爲電子監控或者監視具備第一個要素。而要舉證具備第二要素(高度冒犯)是困難的，因爲無物理空間的侵入(physical invasion)。事實上，近幾年，第二要素已併入第三個要素。因此，隱私侵權訴訟端視員工有無合理的隱私期待。關於合理隱私期待的檢驗，法院又增加了嚴格檢驗的要件—要求此等期待除了主觀外，尚需客觀合理。法院即運用這個主觀/客觀檢驗原則，首先確定員工合理隱私期待的範圍，確定有主觀性質，然後衡量雇主的商業利益與員工的個人利益，確定具有客觀的本質。

多數的案件，雇主透過訂定電子監控政策，排除員工主觀的合理期待；而許多法院的案例顯示，客觀的合理期待又常因工作場所運作的實際需要或商業慣例被推翻[215]。

(2)各州侵權行爲法

員工電子郵件的隱私權保護，早已被各州的侵權行爲法[216]所涵蓋，在侵權行爲法中有四種保護隱私的規定：無故侵入私人空間、盜用他人的姓名或肖像、無故公開他人的生活、在他人未予公開之前先予以公開。和電子郵件較相關的是第一種

[215] Ray Lewis,*Employee E-mail Privacy Still Unemployed: What the United States Can Learn from the United Kingdom*, 67 La. L. REV. 959,964-965(2007)

[216] 在美國，各州可以自由起草侵權行爲法規，支持或否決某些侵權行爲的態樣。同樣地，各州法院組織可以依據該州判例自行解釋該州的法規和判例法。結果，在某些州某些案子可能可以侵犯隱私權爲訴之理由合法起訴，但在某些州卻會被法院駁回。參考，愛倫.艾德曼、卡洛琳.甘迺迪著，隱私的權利，商周出版，2001 年，頁 207。

情形，即無故侵入他人的私密空間（unreasonable intrusion upon the seclusion of another）。侵權行爲一般要求原告必須舉證二個要件：（1）必須對一個理智的一般人構成高度的侵害（highly offensive to a reasonable person）（2）原告有隱私的合理期待（reasonable expectation of privacy）[217]。因此法院在相關案件中，判決電子郵件的監看與一般的電話監聽相似，侵入就足夠成爲侵權行爲的要素之一。在認定是否構成侵害，法院會考量侵入的程度、侵入者的行爲跟環境、侵入者的動機、被侵害隱私的合理期待性等因素，但有明示或默示同意，就不會被認爲侵入。法院在衡量是否會構成侵害隱私權時，法院也會要求是否有客觀的隱私權合理期待存在與此期待性是否合理，當然公司的商業利益也是考慮因素之一[218]。

（二）美國聯邦立法

美國傳統上，憲法與普通法常常無法解決資訊社會中隱私權爭議，所以多透過國會立法的方式針對隱私權議題加以規範。然而，美國聯邦政府關於秘密電子監視的法律規範很少。1986 年的電子通訊隱私權法（Electronic Communication Privacy Act ，ECPA）禁止攔截（interception）、揭露（disclosure）或利用（use）有線、口頭或電子通訊[219]。美國國會曾於 1990 年提出消費者與勞工隱私法（the Privacy for Consumers and Workers Act，PCWA）、2000 年提出電子監控通知法（Notice of Electronic Monitoring Act，NEMA），然而該二法案皆未審查通過。

1. 電子通訊隱私權法（Electronic Communication Privacy Act ，簡稱 ECPA）

---

[217] Benjamin F. Sidbury，*You got mail…and your boss knows it：Rethinking the scope of the employer E-mail monitoring exceptions to the Electronic Communications Privacy Act*，UCLA J. L. TECH. 5（2001）。Ira David, *Privacy Concerns Regarding the Monitoring of Instant Messaging In the Workplace: Is it Big Brother or Just Business?* 5 NEV. L.J. 332-333（2004）

[218] 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，月旦法學第 85 期（2002 年 6 月），頁 97。

[219] National Workrights Institute, Privacy Under Siege: Electronic Monitoring in the Workplace 14 (2005), available at http://www.workrights.org/issue_electronic/NWI_EM_Report.pdf（最後瀏覽日期：2007 年 12 月 17 日）

在美國國內，關於電腦犯罪法規（例如：The Computer Fraud and Abuse Act of 1986）和與資訊隱私有關的聯邦法規並未規範私領域雇主監測雇員電子郵件通信的問題。唯一具體地提及電子郵件通信攔截（interception and accession of E-mail communications）的聯邦法規是電子通訊隱私權法（Electronic Communication Privacy Act ，ECPA）[220]。

爲了回應 1968 年的 Katz v. United States[221] 及 Berger v. New York[222]案，美國國會立法通過 ECPA 第三編（Title III of the Omnibus Crime Control and Safe Streets Act of 1968）適用範圍原先僅限於有線及口頭通訊[223]。

1985 年修正後始擴及包括攔截電子通訊以及未經授權進入儲存的電子通訊[224]。雖然無明確規定，但大部分的美國學者主張，由立法沿革可看出電子郵件爲 ECPA 定義的「電子通訊」。ECPA「攔截」的定義包括任何有線、電子或口頭通訊的內容（the “aural or other acquisition of the contents of any wire, electronic, or oral communication.”）[225]。

ECPA 制定的目的是爲補充 1968 年反竊聽法案（anti-wiretapping act）的漏洞，其因 1960 年代後期的水門醜聞事件，爲反制政府不當的竊聽。在原始的條文中，除非政府調查員取得法院的監聽同意，否則政府不能未經同意即竊聽電話的通話內容。在 1986 年晚期，國會進一步擴張了 ECPA 的適用範圍，使其可及於電子通訊的內容：

---

220 Larry O. Natt Gantt, II, A*n affront to human dignity: electronic mail monitoring in the private sector workplace*, 8 HARV. J. LAW & TEC,351（1995）

221 389 U.S. 347 (1967). The Supreme Court set the threshold for Fourth Amendment protections at whether a reasonable expectation of privacy existed in the area searched by officials.

222 388 U.S. 41 (1967) (extending the ruling in Katz to electronic eavesdropping on oral communications).

223 See 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, 151 n.62 (1994).

224 See 18 U.S.C. 2510(1), (4), (12), (17) (1994).

225 18 U.S.C.2510(4) (1994); see Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994).

1. 規範對象除了電話通訊內容（voice communication on telephone）外，再加上所有數位通訊（all forms of digital communications ），包含文字（text）及數位化的影像圖形（digitized visual images）。

2. 禁止個人或商業上未經授權即非法竊聽，不再單及於政府非法竊聽。

3. ECPA 不光禁止未經過授權攔截通訊中的訊息，也禁止未經授權取得儲存在電腦系統中的訊息資料。

故 ECPA 是第一部能保護人民在電子通訊的傳輸過程及儲存時，免於未經授權的截取、竊聽和洩漏[226]的聯邦法規。

一旦系統管理者侵犯了用戶的隱私權， 例如系統管理者公佈私人的電子郵件內容給所有網路業者閱讀時，ECPA 給用戶三種權利得以控告系統管理者：

1. 用戶有權要求系統管理者移除其被公開的隱私。

2. 用戶有權要求金錢上之損害賠償。

3. 用戶有權要求請求律師費用[227]。

但就EPCA 賦予用戶的三項權利來看， 就第一點而言， 由於訴訟時緩不濟急，即使訴訟獲得勝訴， 隱私受侵害的情形也早已造成。而就金錢賠償而言， 要證明隱私權的侵害造成多大的損害及範圍， 亦是一件十分困難的事。因此， 法律上縱使有這些權利， 但卻即可能發揮不了作用。至於， 律師費的補償方面， 主要是避免受隱私侵害的用戶， 因龐大的律師費用而不對系統管理者提出訴訟，因此， 一旦系統管理者敗訴， 即需支付用戶所支出的律師費用。

a.ECPA 之例外

除侵權行爲法外，ECPA 仍是最能提供電子通訊隱私權保護的法案，但如果雇主具備該法的例外規定，則可免除責任。

ECPA 存在的例外如下：

---

[226] 王郁琦，工作場合中電子郵件隱私權之研究，收於氏著「資訊、電信與法律」，元照出版，2004 年 5 月，頁 95。

[227] ECPA，18..U.S.C.2520（1988）。

（1）商業使用之例外（business use exception）

ECPA 的第一個例外是企業用途例外－允許合法商業目的正常使用。公司電子郵件系統是企業工具，使用這樣一個工具監測雇員的雇主在 ECPA 之下是擁有監看權利的。

（2）提供者之例外（service provider exception）

ECPA 的第二例外是服務提供者例外。根據該條款「電子交換系統的操作者，或是電信、電子通訊服務提供者之受僱人或代理人，若其設施係用來傳遞電信或電子通訊，且在從事任何謂保護提供此等服務提供者權利或財產所相關的活動，其根據業務正當程序而對通訊所爲之截聽、揭露或使用，並非不法行爲」[228]。

因此，若雇主提供網路系統以供員工傳遞電子郵件時，根據提供者例外之規定，在正常業務程序（ in the normal course of employment） 與爲保護雇主權利或財產或提供此等服務所相關（necessary incident）的前提下，即可監看或攔截員工的電子郵件通信[229]。

（3）事先同意例外（prior consent exception）

ECPA 允許通訊雙方的任何一方於事先同意之下，允許中途攔截傳遞中的電子郵件或接觸其儲存的電子郵件內容[230]。在雇主監看公司電子郵件系統的情形，若經員工同意， 雇主將可豁免責任。所謂同意，除明示外，尚包括默示同意。但是，即使雇主證實有明確監看政策，或主張員工默示同意，但員工如果可證實雇主基於犯罪或侵權行爲目的而監視，也許仍然能勝訴。例如，基於強奪、 敲詐等目的[231]。

---

228 "it shall not be unlawful . . . for . . . an officer, employee, or agent of a provider of wire or electronic communication service . . . to intercept . . . that communication in the normal course of his employment…"

229 18 U.S.C. 2511（2）(a)(i)。

230 "it shall not be unlawful under this chapter for a person . . . to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent to such interception."，2511（2）(d)。

231 *See* Meir S.Hornung , *Think before you type: a look at email privacy in the workplace*,11 FORDHAM J.CORP.&FIN.L.138-139（2005）。

（4）ECPA 的最後例外是法院增加的 「同時」（contemporaneity）要求。在 Steve Jackson Games, Inc. v. United States Secret Service 一案中，第五巡迴法院指出，雇主必須在電子郵件在傳輸的同時攔截，才構成違反 ECPA 的規定[232]。之後每個法院幾乎都維持此見解[233]。

但在 2005 年 United States v.Councilman[234][235]案中，第一巡迴法院認爲國會在立法定義電子儲存（electronic storage）時並沒有將此種暫時性儲存（temporary storage）的類型排除在 ECPA 的規定外，似乎暗示想廢棄「攔截」須符合傳輸中的要求之見解[236]。

b.對 ECPA 的批評

ECPA 除了被批評缺乏明確性（lack of clarity）外，法院也認爲個人通信的攔截和監看不屬於商業一般正常使用目的例外（ordinary course of business exception），因

---

232 因爲在 ECPA 的定義中，所謂的攔截包含傳輸中聲音的獲得或其他方式（other acquisition）的獲得，因此在一些法院的解釋中，存在電腦中 e-mail 信件已不在傳輸中。由於 e-mail 本身並非聲音，故無法在聲音傳輸攔截的定義內。

233 *See* Meir S.Hornung , *Think before you type: a look at email privacy in the workplace*,11 FORDHAM J.CORP.&FIN.L.139（2005）。

234 United States v. Councilman,418 F.3d 67,72-77（1st Cir.2005）

235 本案推翻該國法院過去所建立「電子郵件服務提供者未經使用者同意監視使用者電子郵件通訊，不屬違反監聽法之犯罪行爲」的立場。被上訴人 Bradford C. Councilman 是從事珍貴與絕版書籍網路建擋列表服務之 Interloc Inc. 的副總裁，該公司給與其顧客含有"interloc.com" 網域名稱之電子郵件地址作爲服務的一部份，並且提供如同電子郵件服務提供者之服務行爲，本案起因於 1998 年 Bradford 指示該公司雇員透過修改郵件接收程序之方式，攔截並拷貝所有服務使用者與其競爭對手亞馬遜網路書店 (Amazon.com) 間的電子郵件通訊，亦即，所有來自 Amazon.com 的信件到達伺服器時，由於程式的運作，該信件於寄至使用者信箱前會先行複製，由 Interloc 公司員工加以閱讀。上訴法院之判決，乃針對電子郵件的傳送是否屬於監聽法中所謂的電子通訊 (electronic communication) 以及該公司之行爲是否構成「攔截」皆作成肯定之解釋，對於電子郵件使用者隱私權之保護有指標性的影響。參考，http://stlc.iii.org.tw/ContentPage.aspx?i=683 http://w2.eff.org/legal/cases/US_v_Councilman/councilman_decision.pdf http://www.out-law.com/page-6009（最後瀏覽日期：2007 年 12 月 30 日）

236 The court stating" we note ,however, that even were we prepared to recognize a contemporaneity or real-time requirement-a step that we do not take today-we think it highly unlikely that Councilman could generate a winning argument in the circumstances of this case." See Meir S.Hornung , *Think before you type: a look at email privacy in the workplace*,11 FORDHAM J.CORP.&FIN.L.140-141（2005）。

此，論者有認爲 ECPA 第二編（Title II）和第三編（Title III）應明確修正禁止雇主監視個人通訊。否則，法院也無可避免必須承擔確定哪些通訊是與商業有關或是屬於私人的難題[237]。

2. 消費者及勞工隱私法（the Privacy for Consumers and Workers Act，簡稱 PCWA）

因 ECPA 未直接針對接近工作場所電子郵件通訊作規範，加上 ECPA 的案例法提供給工作場所使用者的保護有限。對於工作場所電子郵件通訊的問題在於何時、何種目的下可以接近。

1990 年至 1993 年間美國參議員 Paul Simon 有感於無限制的監控員工已使現代辦公室成爲「電子血汗工廠」（electronic sweatshop），試圖提案訂定消費者及勞工隱私法（the Privacy for Consumers and Workers Act，簡稱 PCWA）。

該法立法目的是爲了透過雇主執行電子監控的通知，以保護員工免於秘密監控。PCWA 賦予勞工「知的權利」--包括監控將於何時、何地實施，並預先通知資料蒐集及如何被利用。該法案規定，雇主須建立政策並通知員工監看的規則。再者，該法案禁止公司儲存、蒐集、利用、散佈電子監看所獲得的資料。

此外，該法案要求雇主實際實施監控時，要有訊號警示（signal light）、警示音（beeping tone）、口頭通知或其他形式的通知。經由 PCWA，即使雇主與員工簽訂電腦與網路使用的協議，該協議也無法剝奪員工基於憲法增補條款第 1 條所享有的言論自由的權利。法案在國會辯論時，參議員 Paul Simon 在當時並指出，美國和南非是唯一未提供員工工作場所隱私保護的國家。

反對者則指出，PCWA 會使侵權行爲法及其他救濟途徑失去原有效用[238]。

---

[237] Benjamin F. Sidbury，*You got mail…and your boss knows it：Rethinking the scope of the employer E-mail monitoring exceptions to the Electronic Communications Privacy Act*，UCLA J. L. TECH. 5（2001）。

[238] Lee Nolan Jacobs, *Is What's Yours Really Mine?: Shmueli v. Corcoran Group and Penumbral Property Rights,,* 14 J.L. & Pol'y 837,863-864（2006）

PCWA 無疑對私領域員工隱私保護邁出一大步，惟有學者批評指出，PCWA 未能充分保障員工隱私利益[239]。該法案最後未能通過。

3. 電子監控通知法（Notice of Electronic Monitoring Act，簡稱 NEMA）

在 PCWA 提案失敗 10 年後，參議員 Charles Schumer 及眾議院議員 Charles Candy 於 2000 年提案訂定電子監控通知法（Notice of Electronic Monitoring Act，簡稱 NEMA）。該法案要求雇主要以電子方式讀、聽或監控員工的有線、口頭或其他電子通訊，應事先通知員工。通知的內容需包括監控如何進行及因此獲得的資訊如何保存。甚且，該法案要求雇主公開監控與蒐集所取得與工作無關的資訊。員工於權利受侵害時，得向聯邦法院請求損害賠償。得請求的最高賠償額達美金 500,000 元[240]。惟本法案亦未能通過。

（三）州法

ECPA 允許各州自行立法訂定規範隱私的相關法規，只要符合 ECPA 的最低標準。多數州僅就 ECPA 略作修改，很少提供較 ECPA 更大的保護。紐約州與麻塞

---

[239] 美國參眾兩院皆提出 PCWA 的版本，本法重點在於課予雇主「通知」義務。惟哈佛大學的 Larry O. Natt Gantt, II 教授批評指出，該法對於電子郵件的保護，仍不周延。理由如下：首先，儘管眾議院的法案版本是爲補充 ECPA 關於電子郵件保護，惟參院版本明確排除”截取有線、電子或口頭通訊[ECPA] “ 。從而，電子郵件，非定義的「電子監控」。再者，無論是美國眾議院或參議院的版本，許可具體監控的基準，視員工的服務年資而定。第三個原因，也是最重要的是，沒有有效限制監控範圍。雇主雖有義務通知員工監控規則（monitoring practices），但在參院的版本，對於服務未達 5 年的員工，仍可自由監控內容與工作有關的電子郵件訊息。眾院的版本則針對所有員工。通知的要求並未加重雇主工作規則的責任，因大部分的員工必須承擔被解僱的風險。此外，允許雇主監控與工作相關的通訊，則與 ECPA 面臨同樣的問題--因爲雇主仍然可自由監察所有通訊內容，以確定他們是否與工作有關或個人（business or personal）。法院也必須承擔決定哪些通信是與工作有關艱難的任務。諷刺的是，PCWA 因此有效地允許了雇主訂立工作規則並進一步免除雇主的侵權行爲責任。*See* Larry O. Natt Gantt, II, A*n affront to human dignity: electronic mail monitoring in the private sector workplace* ,8 HARV. J. LAW & TEC 345,409-410（1995）

[240] Lee Nolan Jacobs, *IS WHAT'S YOURS REALLY MINE?: SHMUELI V. CORCORAN GROUP AND PENUMBRAL PROPERTY RIGHTS,* 14 J.L. & Pol'y 837,865（2006）

諸塞州有相似的法規禁止雇主竊聽及錄音員工在工作場所的談話。但在 *Restuccia v. BurkTechnology, Inc.*案，法院指出，麻州法律並未適用於電子郵件[241]。

2001 年 Delaware 州通過法規要求全部雇主（包含公、私部門），對員工監控實應行通知[242]。該州法規定「雇主不得監控或攔截電話談話內容或傳輸…除非雇主提供某種形式通知」[243]。

通知的形式透過任何一種方式實施 （1）當員工接近電子資源時，每日至少提供一次通知（2）提供員工關於監控範圍和類型的書面通知[244]。該書面通知必須被安全保存，公司和員工各收執一份，並經員工及其監督人同意[245]。

2003 年，Connecticut 州通過「工作場所科技通訊法」（the Communications Technology in the Workplace Act）[246]。康州的法規只允許雇主蒐集透過直接觀察所獲得的活動資訊[247]。雇主被定義爲包含政府及私人[248]。

不過，當雇主實施電子監視時，如就全部的監控形式提供員工書面通知，並且公開揭示，則得被允許[249]。

有學者指出，州法除了缺乏聯邦法律有統一性以外，以州法來消除歧異，並不適當，而且對於工作場所隱私的規範常受到公司遊說團體的強烈反彈杯葛[250]。

（四）契約法

在美國，私營企業員工依契約法應可提供更實際直接的保障。

---

241 Jay P. Kesan, *Cyber-Working OR Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289,301（2002）

242 19 Del. C. 705 (2005).

243 19 Del. C. 705(b) (2005).

244 19 Del. C. 705(b) (2005).

245 19 Del. C. 705(b)(1)(2) (2005).

246 Conn. Gen. Stat. Ann. 31-48d (2005).

247 Conn. Gen. Stat. Ann. 31-48d(a)(3) (2005). Conn. Gen. Stat. Ann. 31-48d(a)(3) (2005).

248 Conn. Gen. Stat. Ann. 31-48d(a)(1) (2005).

249 Conn. Gen. Stat. Ann. 31-48d(b)(1) (2005).

250 Jay P. Kesan, *Cyber-Working OR Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289,302（2002）

契約法的損害賠償訴訟可能起因於個別的勞動契約、團體協商（collective bargaining agreements）、就業政策（employment policies）或工作手冊（manuals）。如果雇主有電子郵件使用政策，承諾員工於工作場所的電子通訊是隱私的，但雇主違反訂定的電子郵件政策，員工理論上應該能成功起訴要求雇主賠償因其違反默示勞動契約（implied employment contract）造成的損害。

默示契約由雇主的某些行爲或口頭承諾產生。例如：某員工爲一家軟體公司工作了 6 個月後遭解僱。他提起不當解雇之訴，訴稱雖無明示的契約約定僱用期限，公司的員工守則使他相信，除非有正當理由，否則他不會被解僱。在訴訟中這種理由會得到法院支持，因爲員工守則的用字遣詞成爲默示契約。一些法院曾裁定雇主違反承諾而解僱員工，雇主可能被判對此非法解僱承擔責任，此在普通法中稱爲承諾禁反言（Promissory Estoppel）。有關針對工作保證做出的承諾，加州最高法院就曾判決一個由紐約搬遷到加州的員工被解僱後可起訴雇主。伊利諾州上訴法院也曾據此理論判決認爲，當雇主向員工表示一個新工作崗位是穩定的，員工因而接受該崗位後，雇主解僱勞工，屬於不當解僱。員工提起此種訴訟必須舉證：第一，雇主曾做出相關表示；其次，該員工信賴此表示，並因此採取某一行爲或沒有採取某一行爲，而此信賴是合理的；最後，此種信賴造成員工損失[251]。但從實務上的經驗看來，關於雇主電子郵件或網路使用行爲監控的案件，員工似乎沒有勝訴的案例。相反地，在 *Smyth v. Pillsbury Co.,*案[252]，法院判決顯示，即使雇主有口頭的承諾，法院認爲員工亦無隱私的合理期待。

（五）勞動法

對美國私部門員工而言，透過聯邦和州勞動法或團體協商（collective bargaining agreements）機制也可能提供另外的隱私權保護[253]。於有工會組織的工作場所，雇

[251] 林晓云等编，美国劳动雇佣法，法律出版社，2007 年 8 月，頁 152-153。

[252] Smyth v. Pillsbury Co., 914 F. Supp. 97, 100 (E.D. Pa. 1996).

主要實施對受僱人就資訊技術使用訂頒政策前，可能被要求與受僱人的工會代表協商。

依國家勞動關係法（National Labor Relations Act ，"NLRA"）[254]規定，

雇主訂定或實質變更工作場所紀律政策是協商的標的。

NLRA 第 7 條[255]規定，員工應有權自我組織、成立、加入或協助勞動組織，透過他們自己選出的團體協商代表，從事為了團體協商或其他其他互助或保護的活動。其中相互幫助或保護（For purposes of mutual aid or protection）已經被從寬認定為包含所有與勞動條件有關的事項。關於此種監控電子郵件的勞動條件及訂定工作規則禁止使用電子郵件通訊，正被討論是否構成「不當勞動行為」（unfair labor practice）[256]。

雖然雇主必須與工會進行協商，但 NLRA 不要求任何一方當事人一定要同意該政策的條件[257]。相反地， NLRA 要求雙方以誠信（in good faith）原則協商[258]，但一

---

253 Edward Lieber, *Picketing The Information Superhighway: Must Employers Bargain With A Union Over Their E-Mail Policy?*, 1998 ANN. SURV. AM. L., 517, 530 (1998) (concluding if email policy is germane to the work environment and not at the core of entrepreneurial control it is the subject of mandatory bargaining).

254 1935 年美國國會頒布，1947 年修正。

255 原文為：Sec. 7. [§ 157.] Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all such activities except to the extent that such right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 8(a)(3) [section 158(a)(3) of this title].

256 William R. *Corbett,The Need for a Revitalized Common Law of the Workplace*，69 BROOKLYN L.REV.91, Fall, 2003

257 美國勞資關係上團體協商之主要法律架構是ＮＬＲＡ第八條Ｄ項之規定。該規定要求雇主與擁有排他協商代表權（排他協商代表，係指某一工會為前述適格的協商單位全體勞工，以秘密投票或非正式票選方式，獲過過半數支持時，該工會即成為該適格的協商單位之惟一的且排他的協商代表，此代表權及於協商單位之全體勞工，縱有不同意見者亦然。）之工會，有就工資、工時及其他勞動條件為相互誠信協商之義務。
National Labor Relations Act (NLRA) defines the duty to bargain as the obligation to "confer in good faith with respect to wages, hours, and the terms and conditions of employment."

258 團體協商中之「誠信原則」是美國法制中獨特之制度。我國現行團體協約法，對於團體協約成立前之協商義務及協商過程中應遵守的規範並無規定。惟 97 年 1 月 9 日修正公布（施行日期由行政院另定）之團體協約法已於第 6 條明定：「勞資雙方應本誠實信用原則，進行團體協約之協商；…」

旦協商達成協議，工會即不得再阻撓該政策的實施。即使員工對於工作場所電子通訊無隱私的合理期待，依據 NLRA，員工可能就雇主何時、如何實施電子郵件監視取得協商談判的權利。

另外，在無工會組織的工作場所，雇主對於電子郵件或者網路使用行爲監視，如果有違法，可能構成被禁止的「不當勞動行爲」（unfair labor practice），可循勞動爭議解決機制處理[259]。

四、美國企業內電子郵件監看相關案例分析

EPCA 雖然就工作場所E-mail 監看的問題做了原則上的規定，但仍非十分明確。其他法律又付之闕如。

對於電子郵件監看，從員工的立場， 其認爲電子郵件屬於其私人財產，信件即應受隱私權的保護， 另一方面公司卻又主張公司電子郵件成立的目的乃爲了公司的商業活動而非私人的用途， 因此公司可以監看。此一爭議即出現了公司的商業利益優先或是員工隱私權重要的利益權衡問題，到底以何者爲優先，法院判決，因而成爲一個很重要的參考資料。從1990年代早期迄今，法院判決產生的問題在一般集中於隱私的合理的期待（reasonable expectation of privacy）、攔截與進入（interception vs. access） 和默示的同意（implied consent）。

關於雇主在工作場所的監控，例如，搜索置物櫃、監控電話或錄像監視原告通常主張侵權行爲法上「侵入隱居之處」。但在電子通訊部分，十多年來，美國法院的多數判決幾乎等於已經宣稱受僱員工在工作場所的通訊沒有隱私的合理期

[259] 美國官方的勞動爭議解決機制由國家勞工關係委員會（National Labor Relations Board，NLRB）主導。它是政府部門中的獨立部門，負責處理工會與雇主間利益上的相互影響關係。它也是 NLRA 的執行機構。它的主要功能有兩個：一是在與雇主交涉的過程中，引導員工就是否被工會會員代表的問題進行無記名投票，即代表權案件；二是預防和補救雇主和工會違反國家勞動關係法的行爲（不當勞動行爲）。參考，林晓云等编，美国劳动雇佣法，法律出版社，2007 年 8 月，頁 176 以下。

待。爲了便於觀察，我們以未預先通知員工的電子監控及經通知的電子監控分類來看這些案例。

（一）未預先通知員工的電子監控

在 1990 年代早期到中期，當公司剛開始監控他們的受僱員工的電子郵件或者上網行爲，相對很少公司有正式的監控的政策。但多數法院判決出乎人意料之外地接受雇主辯稱的，工作場所沒有隱私的合理的期待的說法。

甚至包括未給予將攔截電子通訊警告的情形。這些法院支持電子郵件的監看作爲一個可接受的工作規則（employment　practice）。

1. Flanagan v. Epson America, Inc.[260]

*Flanagan v. Epson America, Inc.*案，是90 年代初期發生員工控告雇主監看電子郵件行爲的案件。本案一群以Flanagan 爲首的公司員工提起民事集體訴訟控告公司侵害其隱私權， 原告主張公司未經其同意所實施的電子郵件的監看， 違反了他們對工作場所的隱私權之期待（ the expectation for workplace privacy）， 法院審理原被告雙方的意見後， 認爲原告Epson 公司的電子郵件系統提供給公司近七百人使用，員工透過密碼來介接到全球的電腦終端機， 雖然ECPA 對於隱私權提供保護， 但是對於公司提供的電子通訊服務，雇主並不對處於儲存狀態的信息負有任何隱私權侵犯的責任。且認爲公司有權管理、維持公司系統[261]。

更令人訝異的是，此加州法院判決認爲電子郵件並非屬於電子通訊（ electronic communication） 的類型， 而無法受到隱私權的保護[262]。

2. Shoars v. Epson America,Inc.[263]

---

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

[261] *See* Ira David， *Privacy Concerns Regarding the Monitoring of Instant Messaging In the Workplace: Is it Big Brother or Just Business?* 5 NEV. L.J. 334-335（2004）。

[262] 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，月旦法學第 85 期，頁 100。

[263] Shoars v. Epson America,Inc. No.BC073243（ Cal.Ct.App.1991）

另一個類似的案子*Shoars v. Epson America Inc.*，在該案中，被告係以美國加州爲基地的Epson America公司，原告認爲公司主管定期的將她對內或對外的電子郵件內容印出並加以閱讀， 嚴重侵犯其個人隱私， 經其向主管反映後， 卻被以將電子郵件帳號從事私人用途的理由遭革職， 因此原告提出了兩項訴訟，一爲不當解僱行爲的個人訴訟， 另一關於隱私權的侵害，認爲公司監看電子郵件違反了加州禁止透過電子媒介監視員工的法律規定的集體訴訟[264]。

加州有嚴格的竊聽法，但並無電子郵件法。原告的律師聲稱電子監視侵犯加州保護傳統通訊型態的法律，特別是電話。儘管電子郵件並沒有特別被提及，但是這是一種藉由電話線傳輸的通訊方式，所以，現行法律應該可以適用。Epson公司則辯稱現行法律只適用於電話，加州議會並沒有特別規範電子郵件，因此他們並沒有違反法律。

結果，受訴法院同意電子郵件不適用加州竊聽法的見解。認爲擴張法律解釋，將電子郵件納入法律規定的範疇，並不是法院應扮演的角色。法院指出，聯邦政府自1986年的「電子通訊隱私法」開始，便致力於解決電子議題，並提供雇主一個特權，依據「電子通訊隱私法」，服務提供者檢查電子郵件，也就是Epson公司在本案中爭執的焦點，並不違法[265]。故這二項訴訟， 原告亦同樣的遭受敗訴的命運。

3. Restuccia v. Burk Technology, Inc[266]

本件麻塞諸塞州的案例是少數顯示雇主監看員工的電子郵件有可能侵犯隱私權的案例。在 ***Restuccia v. BurkTechnology, Inc.***一案中， Restuccia 是 Burk Technology 公司的員工。此公司的主管們可利用監督者的密碼進入公司電腦系統的每一部

---

264 參馮震宇，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，月旦法學第 85 期，頁 101。王郁琦，工作場合中電子郵件隱私權之研究，收於氏著「資訊、電信與法律」，元照出版，2004 年 5 月，頁 102。

265 愛倫.艾德曼、卡洛琳.甘迺迪著，隱私的權利，商周出版，2001 年，頁 430-431。

266 No. 95-2125, 1996 Mass. Super. LEXIS 367 (Mass. Super. Aug. 13, 1996).

份，包括員工的電子郵件， 而電腦系統也會自動將所有的電子郵件存在備份的檔案裡。但員工並不知道高階主管能夠看到他們的電子郵件，也不知道系統會自動把電子郵件備份。在本案，雇主並未訂定電子郵件政策通知員工他們的電子郵件訊息或儲存在電腦的備份檔可能被監控，或禁止員工將電子郵件系統作爲私人通信之用，只有禁止「過度聊天」。員工被提醒要經常更換密碼，但是未告知員工監督者可能接近他們的訊息。

該公司一位經理告訴公司老闆 Burk， 有一員工花很多時間使用電子郵件系統。Burk 用監督者的密碼， 進入備份檔案裡察看員工的電子郵件。他發現 Restuccia 和另一員工 LoRe 在幾封電子郵件中談起 Burk 和另一員工的婚外情。三天後，Burk 將 Restuccia 與 LoRe 解雇， 聲稱解雇的原因是因爲他們違反公司政策，過度使用電子郵件系統，[267]沒有提及他們說閒話的事實。

原告 Restuccia 與 LoRe 提起隱私受侵害的侵權行爲訴訟，主張他們的電子郵件有隱私的期待，因爲他們有個人密碼。本案受訴法院認爲，原告是否有隱私的合理期待（reasonable expectation of privacy），在於老闆閱讀受僱人的電子郵件和是否形成不合理（unreasonable）、實質（substantial）或者嚴重干預（serious interference）原告的隱私。法院認爲，員工可以使用電子郵件系統，來作爲私人通信之用。而且，雇主未告知員工管理階層可透過管理者密碼來存取他們的訊息或員工的電子郵件會被儲存到備份的檔案裏。於此情形下，員工可主張對於私人的電子郵件的隱私權享有合理之期待[268]。

本案原告的勝利，似乎表示法院打算糾正工作場所電子郵件攔截的情況，認爲工作場所電子監視侵犯原告的隱私權。

4. Smyth v. Pillsbury Co.,

---

[267] 參蔡美智，從指尖流失的秘密-談員工電子郵件之監視與加密，網路 vs 法律，資策會出版，第 22 章。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 62。

[268] 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 62。

在*Smyth v. Pillsbury Co.*[269]案中，原告係被告公司的經理，透過公司的電子郵件系統跟其他的主管與員工聯繫，公司曾經一再地保證說所有的員工享有電子郵件通訊不被侵擾的權利， 原告主張其信賴公司的保證，而與上司通信，但幾天後即遭解雇， 因爲該經理被認爲傳送不適當及不具專業水準的評論於電子郵件系統中。原告向法院提出此一非法解僱（wrongful discharge）， 是違反公共政策。此一公共政策是禁止雇主以員工提出隱私權受到雇主的侵犯之申訴爲理由即終止勞動契約， 另外原告引用*Brose v. Piece Goods Shop,Inc.*[270]的判決， 該案法院認爲侵犯隱私權係屬於侵權行爲法第652B條之隱私侵入， 而依侵權行爲法第652B之規定： 故意以實體或其他方式，侵入他人之僻處或隱居的地點， 或侵入於其私人事項或私人關係， 如此侵入於一般合理人之觀點， 爲高度之侮辱（侵犯）者， 行爲人應就其侵害隱私權負責任[271]。

僅管原告提出這些主張， 法院首先認爲本案與 Brose 案不同，當員工自願透過公司的電子郵件系統傳送電子郵件至其主管時，法院指陳儘管有任何通訊將不會被管理者攔截之保證，但仍無合理的隱私權期待。本案法官認爲，攔截這些通訊，不若驗尿及個人財產搜查案例般要求員工揭露任何有關個人的資訊。反而是原告自願透過電子郵件系統傳送不具專業水準的評論，在如此之通訊中，聯邦上訴法院無法發現隱私之利益存在。第二，即使認爲員工之電子郵件內容有合理之隱私期待，法院不認爲一般理性的人（ reasonable person） 會認爲被告攔截這些通訊將被認爲是一個實質且高度的隱私權侵犯。法院認爲員工的電子郵件訊息的攔截

---

269 914 F.Supp.97；1996。

270 963 F.2d 611（3d Cir.1992）。在該案例中，原告拒絕公司對個人驗尿及搜查個人工作場所之要求，因此雇主依據其藥物及酒精政策而將上述原告解僱，據此控告雇主之行爲構成非法解僱。原告主張雇主之藥物及酒精計畫違反美國憲法及賓州法律中所規範之公共政策。聯邦上訴法院聲明檢視賓州法律發現公共政策的證據，其中顯示在特定之情形下，有關於驗尿或個人財產之搜索可能導致非法解僱。請參考，江國慶，對 Michael A. Smyth v. The Pillsbury Company 乙案之分析，收於彭心儀主編，「美國資訊通信法案例評析」，元照出版，2002 年 5 月，頁 247。

271 原文爲：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 highly offensive to a reasonable person.

證明是正確的，因爲公司對防止使用它的電子郵件系統的不適當和非專業性的意見有實質的利益，超過員工電子郵件的隱私利益。

本件判決受到學者嚴厲的批評，且有明顯的瑕疵：本判決將原告的電子郵件通訊是否有隱私合理期待的問題，置於分析該電腦是否供全公司使用，並且認爲，當原告經由公司電子郵件系統寄出電子郵件，即喪失所有隱私的期待。法院顯然混淆了「隱私」（privacy）與「隱居之處」（solitude）的概念。即使原告使用雇主提供的電子郵件系統，亦不能排除他有隱私的主觀期待。如果參考第 11 巡迴法院於 ***Walker v. Darby*** 案[272]所表示的見解，主觀隱私期待非僅依據工作場所通訊有無被攔截的危險判斷，而是依據員工是否主觀相信攔截將不會發生[273]。

5. McLaren v. Microsoft Corp.[274],

在 *McLaren v. Microsoft Corp* 案，一位微軟公司的員工控告微軟公司爲了調查內部性騷擾和存貨短缺進入他的電子郵件信箱個人收件匣（personal folders），閱讀他儲存在電腦上寄送給第三者的檔案夾的內容。微軟公司的前雇員聲稱當微軟公司允許他有個人檔案夾的網路密碼，他有隱私的期待，故主張微軟公司有意不合法侵犯隱私。

然而，*McLaren* 法院忽略本案員工有公司授權設定的密碼和該檔案標明「個人」，而認爲，電腦是雇主的財產和辦公室環境的一部分。此外，法院指出，儲存在原告的個人檔案夾的電子郵件訊息，已經過網路傳輸並且第三者易接近。 因此，認爲原告就該檔案沒有隱私的期待，即使已標明是私人的。

McLaren 法院也將個人電子郵件檔案夾與有隱私期待的儲物櫃搜索作區分。

法院推論，員工以儲存個人物品的具體目的而被發給置物櫃，而原告的電腦僅因

---

[272] 911 F.2d 1573 (11th Cir. 1990).

[273] *See* Rod Dixon，*Windows Nine-to-Five: Smyth v. Pillsbury and the Scope of an Employee s Right of Privacy in Employer Communications*，2 Va. J.L. & Tech. 4，1997.

[274] No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (Tex. App. 1999).

就業的原因被提供。

法院指出：即使原告把電子郵件訊息移到個人檔案夾，任何儲存在他的個人檔案夾裡的電子郵件消息經過網路傳輸，使得第三者容易接近，鑑於這些情形，我們不能因 McLaren 設定個人密碼，即證明原告發送微軟公司經公司禁止的電子郵件訊息內容有隱私的合理期待[275]。法院斷定即使他就公司的電子郵件系統有隱私期待，對電子郵件的攔截也非對一個講理的人造成高度冒犯，因此可能沒有侵權行爲法之「侵入他人隱居之處」（intrusion upon seclusion）。

（二）基於通知的電子監控

越來越多的雇主訂定電子郵件和網際網路使用政策，以保護他們的無形資產並且降低訴訟機率。 一項 2004 年的研究指出，百分之七十九的雇主實施書面電子郵件政策[276]。 當公司實施電子郵件或網際網路使用政策，它實際上的目標是爲消除員工基於電子通訊監控的隱私侵害損害賠償請求。

1. Bourke v. Nissan Motor Corp[277]

發生於加州的*Bourke v. Nissan Motor Corp*案，原告是受雇於Nissan公司的2個客戶服務人員Bonita Bourke與Rhonda Hall，他們的主管會印出他們的電子郵件來看，在其中發現不適當的笑話及言語（含有色情相關內容），便予以警告，該2名員工在接到警告後，便向公司表示對監看行爲的不滿，亦被公司免職。因此提起訴訟，

---

275 原文爲：Even [if the plaintiff's practice was to move e-mail messages to personal folders], any e-mail messages stored in McLaren's personal folders were first transmitted over the network and were at some point accessible by a third-party [because they were temporarily stored in the central routing computer accessible to the employer]. Given these circumstances, we cannot conclude that McLaren, even by creating a personal password, manifested - and Microsoft recognized - a reasonable expec-tation of privacy in the contents of the e-mail messages such that Microsoft was precluded from reviewing the messages.

276 American Management Association, 2004 Workplace E-Mail and Instant Messaging Survey (2004), available at http://www.amanet.org/research/pdfs/IM_2004_Summary.pdf;
American Management Association, 2003 E-mail Rules, Policies and Practices Survey (2003), available at http://www.amanet.org/research/pdfs/Email_Policies_Practices.pdf.

277 No. B068705 (Cal. Ct. App. July 26, 1993), available at http://www.law.seattleu.edu/fachome/chonm/Cases/bourke.html.

聲明公司從事不法的電子郵件監看，並因此解僱他們，這種行爲侵犯隱私權。但Nissan汽車公司員工被要求簽署切結書，說明他們理解Nissan的電子郵件政策是限制使用電子郵件是基於商業目的。本案被告公司提出公司與員工事先已經簽訂了監看契約，本案中被告公司提出公司與員工事先已經簽訂了監看契約，法院也也認爲原告意識到公司的系統管理員有權閱讀他們的郵件。員工既知道公司的監看政策，該員工對於其電子郵件無隱私權合理的期待，法院因而判員工敗訴。

2. Garrity v. John Hancock Mutual Life Insurance Co. [278]

本案二名在Hancock人壽保險公司長期工作多年的員工因有其他員工向管理者抱怨原告轉寄網路性笑話給第三人而被解僱。

法院發現該公司的電子郵件政策禁止「性、誹謗、濫用、猥褻、褻瀆上帝或者種族仇恨及威脅攻擊的訊息。」

被解僱者聲稱，電子郵件政策並未於公司的內部網路系統（intranet system）公告。他們並表明該公司發送的通知函並未明確傳達該公司的電子郵件政策。 不過，法庭認定原告寄送的電子郵件違反被告的電子郵件政策。Hancock 法院認爲原告他們透過雇主的電腦系統上傳送的電子郵件沒有隱私的合理期待。法院承襲 ***Smyth v. Pillsbury Co.***案的見解，認爲員工自願使用公司公司的電子郵件系統即失去隱私的合理期待，至於公司是否有電子郵件政策不重要。 更進一步，法院說明雇主的利益比原告的隱私利益重要。

3 Thygeson v. U.S. Bancorp [279]

本案一位爲被告公司工作 18 年的員工因違反公司的網際網路使用政策未經給付退職金即被解僱。

公司的工作手冊只是說明員工不得使用公司電腦資源作爲個人目的使用。

---

[278] No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002).
[279] No. CV-03-467-ST, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004).

在另外一個被告的工作手冊警告：不要進入不適當網站，不要發送冒犯（offensive）、 威嚇（intimidating）、敵意（hostile）或違反公司政策的電子郵件。公司保留於有正當商業目的原因監控受僱員工的電子郵件和電腦檔案，包括有合理的懷疑員工違反公司的網際網路政策。

公司估計被解僱的員工，每天花費超過 4 小時瀏覽與工作不相關的網站。

該公司並揭露儲存於公司電腦系統--包含裸露的圖片的不適當的電子郵件和性笑話。原告被解僱，他也正式提出對該公司侵犯隱私以及違反聯邦「受僱者退休收入保障法[280]」（Employee Retirement Income Security Act ，ERISA）的損害賠償訴訟。就退休金部分，法院駁回原告的請求，因他尚未用盡行政救濟途徑。針對隱私的侵犯，法院則認爲，公司接近原告儲存於公司網路的「個人」檔案夾及瀏覽網址的紀錄，原告沒有隱私的合理期待。本件法院甚至認爲，如果在 *McLaren* 案，認爲員工對於儲存於公司電腦上的電子郵件訊息沒有隱私的合理期待。那麼，本件該被解僱員工僅於檔案標示「個人」，甚至沒有建立個人密碼，當然沒有隱私的合理期待。

（三）案例分析

（1）雖然加州州憲法確立隱私權爲該州公民的基本權利，但由上述 *Shoars v. Epson America,Inc.*案、*Flanagan v. Epson America, Inc.*案（未經預先通知監控）及 *Bourke v. Nissan Motor Corp*（經通知的監控）的案例看來，法院都沒有站在員工這一方，在 *Epson* 的案例中，法院拒絕擴張加州法律（加州有類似 ECPA 的竊聽法）[281]的解釋到文字型態的電子郵件上。因爲這個法規看來只適用於語音的訊息，如果要擴張至電子郵件的話，則需要州議會決定，法院認爲應由立法解決，因此原告的主張被法院否定。在 *Nissan* 的案例中，法院的重點在於，公司有一份

[280] 1974 年之「受僱者退休收入保障法」（ERISA）是重要的聯邦勞工法之一，該法明定，受僱者行使該法所保障之權利時，除非另有其他正當理由，否則雇主不得任意解僱。有關美國法上不當解雇之概念及相關救濟，可參考，焦興鎧，美國法上不當解雇之概念及其救濟之道，美國研究第 18 卷第 2 期（77 年 6 月）。

[281] Shoars 案原告依 California Penal Code 631 提起訴訟。

對於公司系統詳細說明的文件，其中有提到在電腦系統中的使用上僅限於公司事務，而這份文件員工是有簽名過的；此外，員工在這個事件發生之前就有注意到公司有監看電子郵件通訊的行爲。就算員工爭論公司必須讓員工保有自己密碼的權利，但法院未將此證言認爲有合理隱私期待，反而認爲，這是一種基於安全上考量的手段，公司爲了保護系統的安全，必須採取這樣的行爲來防止外來者的侵害[282]。

（2）由上述案例的分類觀察，我們也可發現，於雇主未訂定電子郵件使用政策且未預先通知監看的情形，除*Restuccia v. Burk Technology, Inc*案外，即使員工有個人密碼且員工可使用電子郵件系統作爲私人通信之用或員工已於檔案標明「個人」的情形，法院除了有認爲電子郵件非法規所規範的電子通訊類型、有基於電子郵件容易爲第三人接近的特質，認爲電子郵件無隱私的合理期待外，主要的邏輯似乎是：基於雇主財產權的立場，認爲雇主有權維護其電腦系統、雇主擁有系統所有權，則儲存於其上的文件亦有所有權。並依此推論出：員工就電子郵件訊息內容無隱私的合理期待；對電子郵件的攔截也非對一個講理的人造成高度冒犯，因此可能沒有侵權行爲法之「侵入他人隱居之處」（intrusion upon seclusion）。

（3）於雇主已訂定電子郵件使用政策的情形，多數法院判決認爲，員工既知道公司的監看政策，自願使用公司電子郵件系統，或已同意簽訂同意書，對電子郵件即無隱私的合理期待。關於電子郵件政策於監看的範圍、合理性、明確性、比例原則等均未探究。於簽訂同意書的情形，亦未考量該勞動契約是否合乎誠實信用原則。由上開案例看起來，美國在隱私的保護似遠低於該國對於言論自由的保障。

---

[282] 參馮震宇，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，月旦法學第 85 期，頁 101。王郁琦，工作場合中電子郵件隱私權之研究，收於氏著「資訊、電信與法律」，元照出版，2004 年 5 月，頁 102。

美國機械性的判決基於財產權的理論，認爲既然商業電腦是雇主的財產，雇主有自由監看的權利。如果我們由 *Garrity v. John Hancock Mutual Life Insurance Co.*案那些接近原告退休年齡的原告聲稱，其他人濫用公司電腦系統，並未遭解僱，公司一直要找到解僱他的理由來看，不免產生該監看權利賦予雇主以此解僱員工而免於支付退休金或者退職福利金動機的疑慮。

（四）美國學界批評

（1）**工作場所電子郵件與其他形式通訊的異同**

根據*Smith*法院見解，當員工自願透過公司電子郵件系統傳送郵件將無隱私的合理期待[283]。因此任何電子郵件將不受任何隱私的期待影響。

電子郵件爲電子通訊方式與傳統通訊設備形式不同，但員工的隱私的合理期待與電話或者信件並無不同。大多數法庭認爲監聽員工的私人電話將構成對隱私的侵犯[284]。

事實上，就雇主而言，員工電子郵件更容易進入（接近），不應該是拒不給予員工隱私權的原因。也不應該給雇主以隱密監看或經通知即可監看員工電子郵件的權利。

法庭已經認爲雇主不能開拆寄至員工工作場所的私人信函[285]。

在*Vernars v. Young*案[286]，法院認爲雇主閱讀員工的個人郵件，構成普通法上侵入他人隱居之處。本案例顯示，個人郵件，即使是在工作場所也有隱私的合理期待。

---

283 *See Smyth*, 914 F. Supp. at 101.

284 *See* Hamberger, 106 N.H. at 112.

285 *See Doe II*, 866 F. Supp. at 196 (holding that a jury could find an intrusion upon seclusion where an employer surreptitiously opened, copied, read and resealed employee's personal mail at the workplace). Even where the employer had established a practice of opening workplace related mail addressed to the employee, opening personal mail was forbidden and could be found to be an intrusion upon seclusion by a jury.

286 Vernars v. Young, 539 F.2d 966 (3d Cir. 1976). (holding that private individuals have a right to a reasonable expectation that their person mail will not be opened and read by any unauthorized person).

我們也可以推論出，這種侵犯隱私的行爲是「對一個講理的人有高度的冒犯」。然而，法院並沒有將上述思考方式，適用到電子郵件[287]。

在*Vernars v. Young*案，法院指出「正如同個人就電話通訊不被監控有隱私的合理期待一樣，對於信函未被授權不受開拆也有合理隱私期待」。但很少法院承認電子郵件與傳統的郵件的相似性[288]。法院指出電子郵件容易可接近（進入），降低了隱私的合理期待，所以要主張隱私的合理期待要有更高的標準。但批評者認爲，加密電子郵件與傳統封緘信函基本上相同。如果雇主攔截電子郵件，侵犯員工的隱私可能負侵權行爲責任[289]。

此外，法院也認爲事實上員工使用的電腦是公司財產，因此，包括員工傳送出的電子郵件也是公司財產。

在*McLaren*案，法院認爲本案與*Trotti*案不同，*Trotti*案中置物櫃主要存放個人所有物，非公司物品。相反地，微軟公司提供*McLaren*的網站（workstation）是爲了執行工作的目的，給*McLaren*收發電子郵件。因此，包含在公司電腦上的電子郵件不是*McLaren*的財產，僅是辦公室環境的一部分[290]。

（2）侵權行爲要件的檢討—合理的隱私期待 vs 對理智的一般人構成高度侵犯

「合理的隱私期待」與「對理智的一般人構成高度侵犯」是侵權行爲的兩個標準。

1. 合理隱私的期待

大多數員工意識到公司使用防火牆，阻止他們進入某些網站，使用加密軟體，使用密碼保護重要的資料。而且，網際網路使用者被經常提醒資訊安全的重要：他

---

[287] Todd M. Wesche, *Reading Your Every Keystroke: Protecting Employee E-mail Privacy*, 1 J. High Tech. L. 101,112（2002）

[288] *See, e.g., Smyth*, 914 F. Supp. 97 (holding that the employee had no reasonable expectation of privacy in the e-mail because the employee made the comments voluntarily over the company e-mail system to his supervisor, and because the company owned the equipment).（該判決認爲員工對電子郵件沒有合理的隱私期待，因爲員工自願使用公司的電子郵件系統且公司就該系統設備有所有權)

[289] Todd M. Wesche，*Reading Your Every Keystroke: Protecting Employee E-mail Privacy*，1 J. HIGH TECH. L. 117（2002）.

[290] *See McLaren*, 1999 Tex. App. LEXIS 4103 at 1. *See also Smyth*, 914 F. Supp. at 101.

們瀏覽的網站和他們的雇主經常透過網站聲明線上隱私權政策和免責聲明。也知道駭客和病毒的威脅資訊安全。但雇主花費保護措施不一定意味著員工沒有隱私的合理期待。

很多法院的結論認爲電子通訊內沒有隱私的合理期待是荒謬的。正如同員工的私人郵件或者監聽員工在工作場所的私人電話，或者檢查員工的置物櫃是不允許的一樣，當員工知悉或者可得知悉公司監看電子郵件時，員工應該有合理隱私期待。

2. 對理智的一般人構成高度侵犯

「入侵」要件應該是原告員工更容易主張的標準。正如住宅的侵入，或許隱私的期待存在於屋主心中，但實際侵入時，當然是對一個理智的人構成重大冒犯。同樣，當私人機構員工可能知悉那他們的電子郵件可能被監看，特別是以秘密的方式監看，而實際上發生在他們身上，當然構成侵犯。但在*Smyth*、*Bourke*和 *McLaren* 案，法院認爲電子郵件的電子通訊本質，使電子郵件不具隱私的合理期待。法院顯然忽視了現代科技技術已經允許員工在距離辦公室很遠的家中工作。依目前法院判決的邏輯，可能將擴張到允許雇主監控員工的私人時間生活，僅因爲他們在家中的一台工作場所的電腦上工作。當然，雇主對於員工在工作場所行爲也必須負擔侵權行爲的連帶賠償責任及必須保護他們的智慧財產權以防止商業間諜或者駭客。不過，不能以員工的隱私權作爲代價[291]。

第四節　　結語

費茲傑羅（Scott Fitzgerald[292]）的「偉大的蓋茨比」（The Great Gatsby，中譯：大

---

[291] Rebecca Ebert，*Mailer Daemon: Unable to Deliver Message Judicial Confusion in the Domain of E-Mail Monitoring in the Private Workplace*，1 J. HIGH TECH. L.81-83（2002）

[292] 費茲傑羅有「爵士年代的桂冠詩人」的稱號，1925 年，他最著稱的作品《大亨小傳》出版後，海明威與 T.S.艾略特皆曾給予極高的評價，此書更在美國「現代文庫」的 20 世紀百大英文小說中，名列第二。關於費茲傑羅的生平，可參，亞瑟・麥茲納(Arthur Mizener)著，楊惠君譯，費茲傑羅，貓頭鷹出版社。

亨小傳）被譽爲是「偉大的美國小說」，因爲它傳達了「爵士年代」（Jazz Age[293]）的典型情調。小說的第 2 章，費茲傑羅描述了一個戶外大型廣告牌。被遺忘的廣告上沒有臉龐的兩隻大藍眼睛無神地端詳籠罩灰色塵土的垃圾場。在今日科技時代正可用來象徵現代電子化工作場所隱私的流失。廣告招牌上醫學博士 Eckleberg 的藍眼睛現在鎖定勞工。工作場所的網路管理員不分青紅皂白地複製、瀏覽檔案，讀電子郵件、分析鍵盤的輸入，甚至重新寫入密碼。網際網路無可避免地造成電子血汗工廠（electronic sweatshop），在那裡，勞工毫無隱私。電子郵件監看腐蝕員工隱私，並且造成壓力，對身心健康造成負面影響。美國隱私權概念是從 1890 年起提出，但科技發展，持續侵犯個人的隱私。作爲一個旁觀者，本文以爲，美國法律應該對此作出回應：除了修正 ECPA，或另外立法外，普通法應創造新的侵權行爲類型。

當然，美國制度最根本的癥結點，在於該國傳統上對隱私採財產權取向的結果。在下一章我們將由歐洲觀點來比較討論。

[293] 1920 年代的美國一般稱爲爵士年代。