第一章 緒論

第一節 問題提出

第一項 網路垃圾郵件問題

壹、氾濫嚴重性

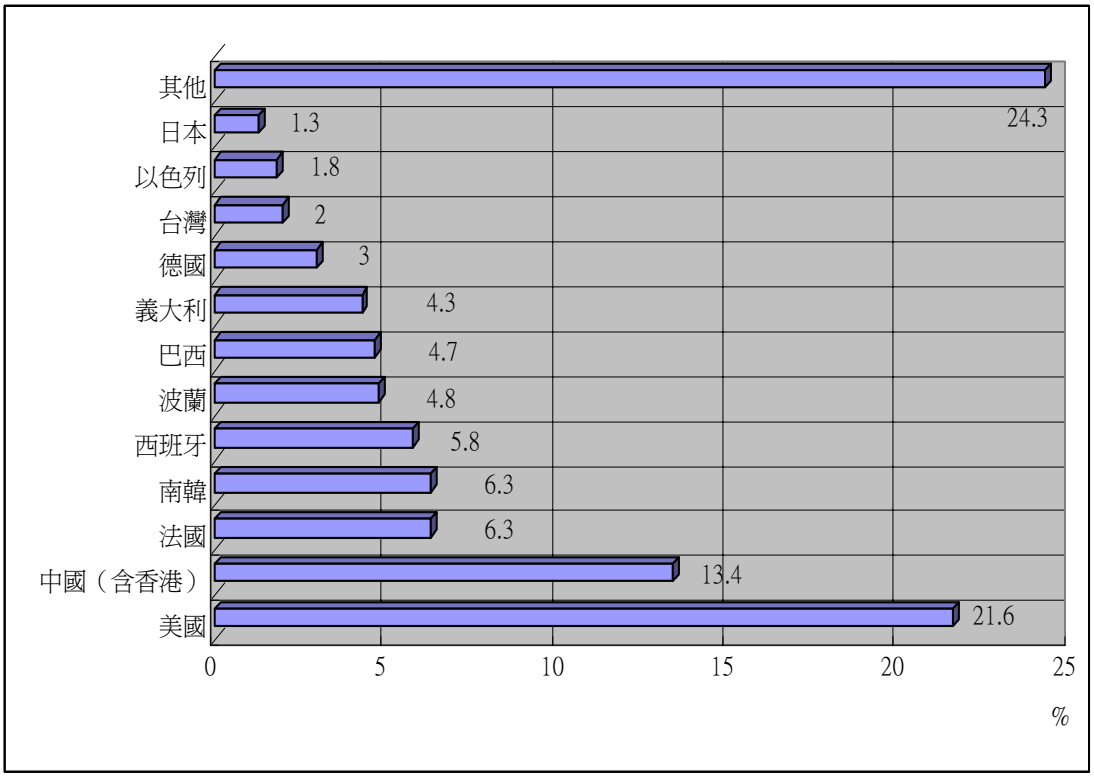
當每天連上網路收信的時候，往往會發現重要的信件早已被為數不少未經邀約（unsolicited），俗稱「垃圾信、垃圾訊息（SPAM）」的郵件所淹沒，網路使用者必須花費不少的時間與精力在刪除垃圾郵件上。根據網路郵件及網路安全設備廠商 Barracuda Networks「2007 年度垃圾郵件調查報告[1]」結果分析顯示，從該公司全球 50,000 個客戶每天 10 億封以上的郵件訊息中，發現 2007 年將近 95% 的郵件是垃圾郵件，比 2006 年增加了 10 個百分點，而 2001 年估計的量僅為 5%而已，有三成的人每天收到超過 10 封垃圾郵件，約一成五的人收到 50 封以上垃圾郵件。另一家防毒軟體公司賽門鐵克於 2007 年 12 月 25 日公布之研究報告亦指出，2007 年 11 月份的垃圾郵件流量持續上升，已經達到歷史新高，整體垃圾郵件在 SMTP 層的比例升高至 72%，幾乎每 4 封信就有 3 封是垃圾信[2]……。

另外，台灣在「網路垃圾郵件發信來源國」的不名譽排行榜上亦佔有一席之地，例如 2006 年 11 月底由歐盟執委會（European

[1] 請參照 http://www.barracudacentral.com/index.cgi?p=spam（最後瀏覽日期 2008/06/30）

[2] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Spam_Report_-_December_2007.pdf （最後瀏覽日期 2008/06/30）

Commission）提出的報告指出[3]，台灣在十二個主要的垃圾郵件來源國中，竟名列第十，占全球垃圾郵件發信總量的百分之二！



圖表 1 網路垃圾信主要來源國家占全球總量百分比圖[4]

貳、手法惡質性

更令人頭痛的問題是隨著網路頻寬與科技的進步，各種發送垃圾郵件的手法也隨之「升級」，且隨時會有創新手法出現，使得網路使用者無法預見。除了最陽春的廣告信件之外，目前網路上流行發

[3] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/1629&format=HTML&aged=0&language=EN&guiLanguage=en（最後瀏覽日期 2008/06/30）

[4]數據資料來源：歐盟執委會 2006 年報告，筆者製圖 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/1629&format=HTML&aged=0&language=EN&guiLanguage=en （最後瀏覽日期 2008/06/30）

送垃圾信的手法，主要有：

一、網路釣魚郵件[5]：

網路釣魚郵件（又稱為 phishing），係指發信者利用垃圾郵件的管道，發送仿效知名網站的電子郵件，引誘無知的使用者進入「偽裝」的知名網站，藉此騙取使用者帳號、密碼或姓名、地址、電話及信用卡等資料，然後再利用這些資料獲取不當利益。至於網路釣魚的誘餌則是五花八門，包括資料過期、無效需要更新，或者是基於安全理由進行身分驗證，騙取個人帳號與密碼，或使用者已中獎（此為「利誘」）等等。

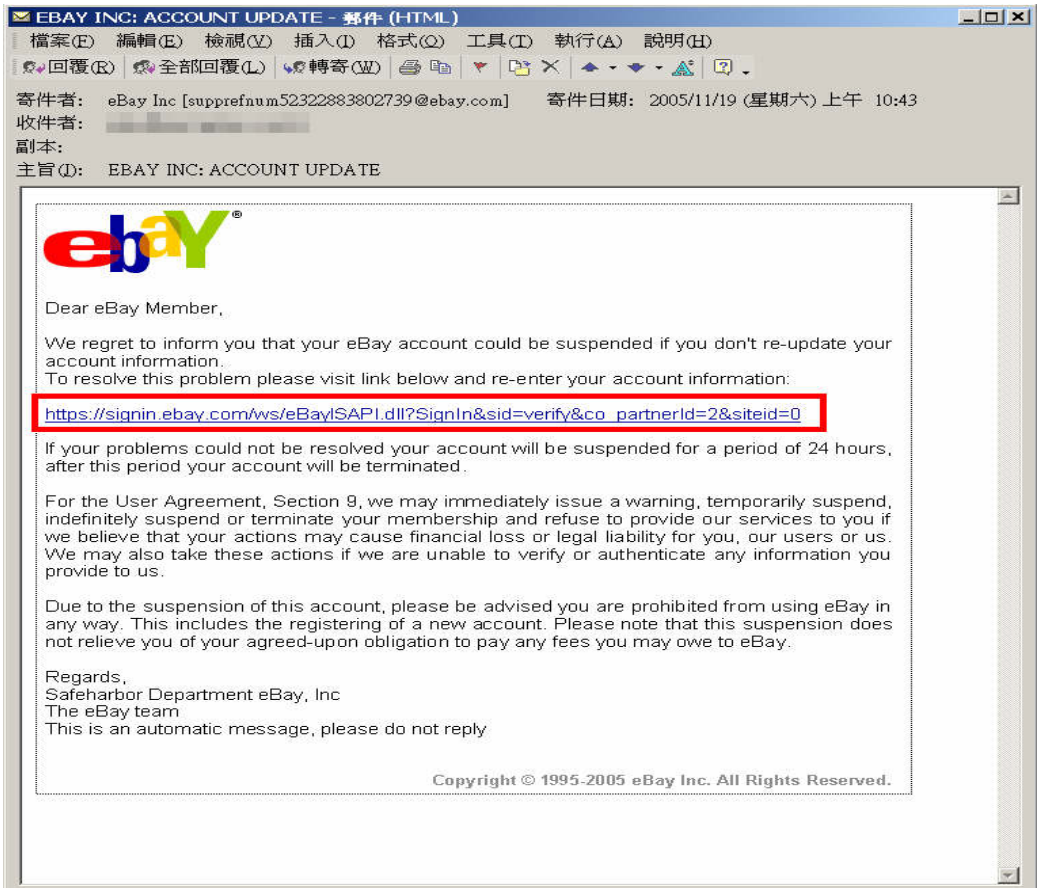
此外，網路釣魚郵件更是不斷「推陳出新」，而又有所謂「魚叉式網路釣魚（Spear phishing）」，係指僅針對特定目標進行攻擊的網路釣魚攻擊。當進行攻擊的駭客鎖定目標後，會以電子郵件的方式，假冒某公司或組織的名義寄發難以分辨真偽之檔案，誘使其員工進一步登錄帳號密碼，使攻擊者得藉機安裝特洛伊木馬或其他間諜軟體，竊取機密；或於員工時常瀏覽之網頁中值入病毒自動下載器，並持續更新受感染系統內之變種病毒，使使用者窮於應付。由於魚叉式網路釣魚鎖定之對象並非一般個人，而是特定公司、組織之成員，故受竊之資訊已非一般網路釣魚所竊取之個人資料，而是其他如智慧財產權及商業機密等高度敏感性資料[6]。

---

[5] *See* Meyer Potashman , *Internationalspam regulation & Enforcement : Recommendations following theworld summit on the information society Y*,29B.C.Int'l&Comp.L.Rev.323,326(2006)

[6] http://www.nytimes.com/2005/12/04/business/yourmoney/04spear.html?pagewanted=1&ei=5088&en=2f313fc4b55b47bf&ex=1291352400&partner=rssnyt&emc=rss（最後瀏覽日期 2008/06/30）

典型且常見的網路釣魚郵件，如下圖所示：



圖表 2 網路釣魚郵件圖

二、偽裝身分垃圾郵件(Email spoofing)：

偽裝身分垃圾郵件是許多垃圾信發送者常用的伎倆，在主旨標題下手，透過偽造個人、政府、銀行或是公司的寄件者名稱來取得收件者的信任感，收件者鬆懈了警覺心而打開這封信件，進而在信件內填入相關個人資料導致被詐騙集團利用。

三、字典式攻擊：

字典式攻擊為 Dictionary attack 的直譯，垃圾郵件的發送者挑選一些常見的英文單字，與其他數字、符號、關鍵字重新組合，

或用程式自動生成電子郵件地址，再將組合過後的文字當作收件者的電子郵件地址，全部一起寄出，例如：

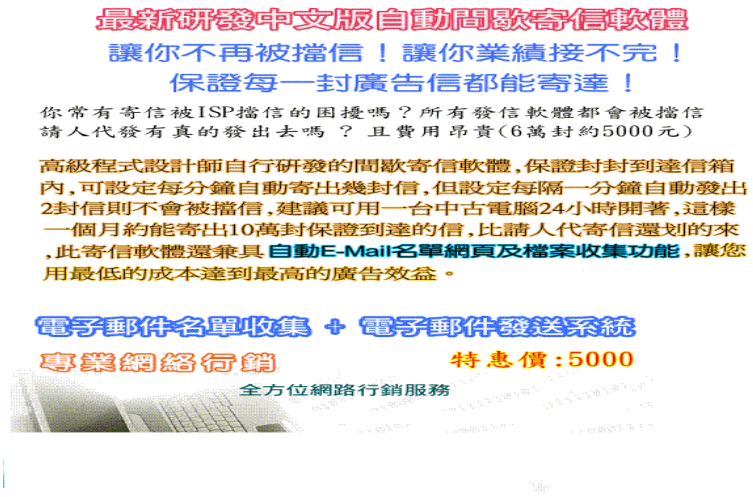
apple@example.com

apple01@example.com

apple02@example.com

apple99999@example.com

發信者通常會挑選擁有使用會員人數最多的電子信箱服務提供者，因為這樣一來「字典式攻擊」的命中率會相對提高。網路上也常見到兼具自動蒐集電子郵件地址與字典式攻擊功能軟體的兜售，如下圖所示：

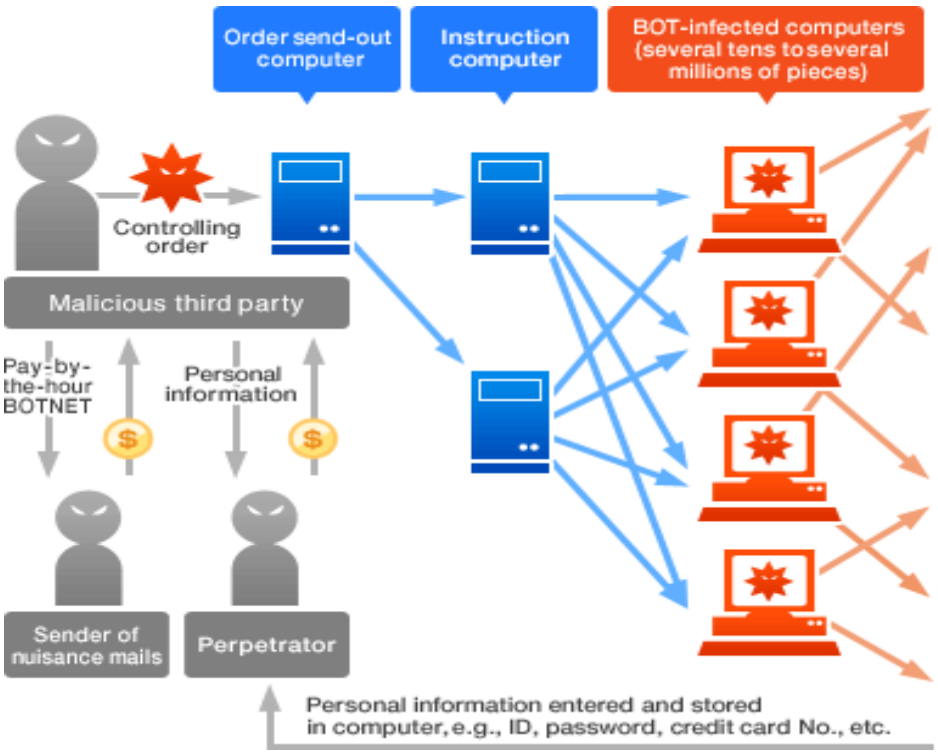


圖表 3 兼具自動蒐集電子郵件與字典式攻擊功能軟體之廣告[7]

[7] 圖片來源：作者電子郵件信箱收到的商業電子郵件

四、僵屍網路

僵屍網路英文為「BotNet」，是機器人網路（Robot Network）的簡稱，又稱「殭屍網路」（Zombie Network），有時又叫傀儡程式。受 BotNet 感染的主機，將如同傀儡般任由控制者操控，以遠端控制受感染的主機，進行網路攻擊，包括竊取私密資料、網路釣魚（Phishing）、散布垃圾郵件（SPAM）等[8]。



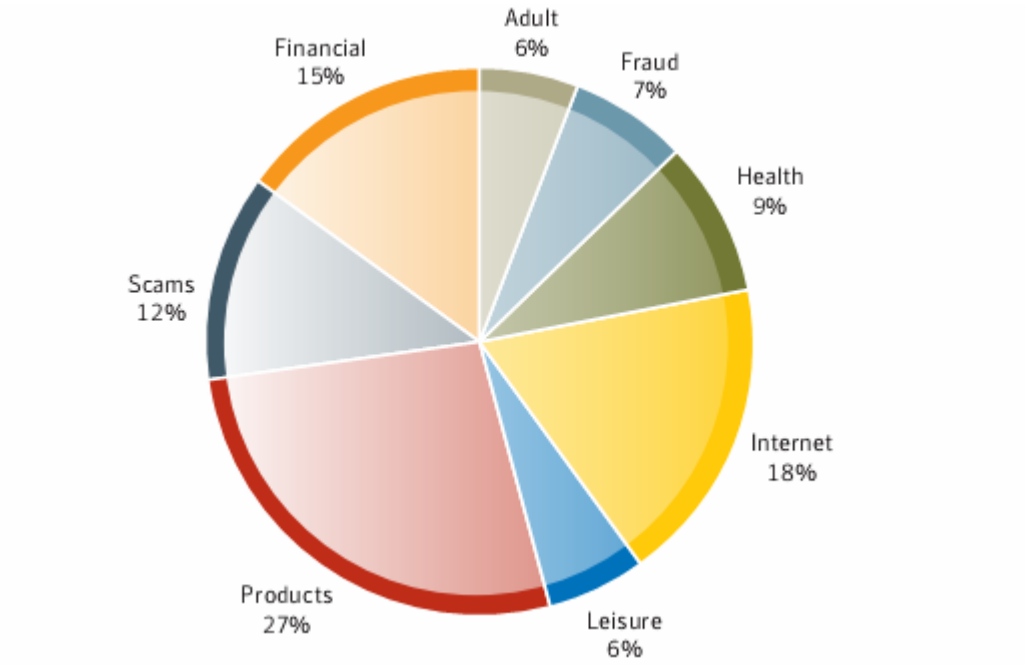
圖表 4　Botnet 示意圖

參、內容多樣性

垃圾郵件的內容可謂五花八門，網路發展初期，礙於頻寬限制，以純文字的型態為大宗，但隨著頻寬的發展與過濾軟體的進步，垃

[8] 圖片來源：https://www.ccc.go.jp/en_bot/index.html（サイバークリーンセンター）（最後瀏覽日期 2008/06/30）

圾郵件內容已經演進為圖片、影音為主；而內容則包含商品宣傳、色情與猥褻圖片影音、傳達宗教思想、候選人拜票、政黨宣傳、詐欺取材……等。以 2007 年 12 月份的垃圾郵件內容為例，得以下圖表示之：



圖表 5　2007 年 12 月各種垃圾郵件內容比例圖[9]

以上資料所舉數據，均足以說明當前網路垃圾郵件氾濫問題的嚴重性，若將網路垃圾郵件稱為網路使用者之「公敵」，相信亦不為過。垃圾郵件的氾濫除了占用頻寬，造成 ISP 業者經濟上損失外，使用者也因此必須花費時間刪除信件，降低其使用網路之意願；惡質的發信手法，導致個人資訊洩漏，甚至形成犯罪等社會問題；內容為色情、猥褻影音的郵件，則對於未成年人身心健全成長有所危

[9]請參照賽門鐵克公司調查報告，
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Spam_Report_-_December_2007.pdf （最後瀏覽日期 2008/06/30）

害……等，對於網際網路科技的發展絕對是百害而無一利。

第二項 各種解決途徑嘗試

對於垃圾郵件氾濫嚴重的問題，各國政府與網路使用者均不斷地尋求各種解決之道，包括以下幾種途徑[10]：

壹、科技途徑

主要以過濾（filtering）技術研發為主。最常見的為建立黑名單(Black lists)，惟最大缺點在於往往會將收件者一般的電子郵件也阻擋在外無法接收。又如建立白名單（White list），利用使用者自己建立的電子郵件地址清單來過濾所有對使用者發送的電子郵件，只要該電子郵件地址不在許可清單當中使用者的個人信箱就不會收到該電子郵件。不斷地研發「擋垃圾信程式」也是方法之一，例如YAHOO 提供的「垃圾信剋星」、「信箱分身」等。然而，通常發信者會予以破解，使得程式無法發揮功能。

此外，亦有提供所謂「拋棄式電子郵件地址」服務的網頁[11]。拋棄式電子郵件地址是實際電子郵箱位址的轉向，並且有一個有效期限，在有效期限前寄到拋棄式電子郵件地址的信件，將全部被轉寄到實際電子郵件地址；當有效期限一過，這個臨時產生的電子郵件地址就會立刻被系統移除。

---

[10] *See* Meyer Potashman, *International spam regulation & Enforcement: Recommendations following the world summit on the information society, Y,*29B.C.Int'l&Comp.L.Rev. 323,329(2006) 相關的中文文獻請參照王郁琦、陳炳全，〈濫發網際網路廣告信相關法律問題之研究〉,《月旦法學雜誌》，2002 年 2 月，頁 157。《濫發電子郵件行爲之管理與法制規範研究》,行政院經濟建設委會委託太穎國際法律事務所辦理期末報告，2003 年 12 月 31 日，頁 17-34。

[11] 例如 APINC (非商業的網際網路組織)- Jetable.org 自 2003 年 6 月起提供的拋棄式電子郵件服務網頁：http://www.jetable.org/zh/index

貳、市場途徑

例如提高電子郵件使用成本、發行電子郵票等。

參、法律途徑

包括 ISP 業者與網路使用者間的契約規定[12]與政府以立法方式介入管制。

不過明顯地，網際網路垃圾郵件氾濫的問題並非能夠單以科技的力量或市場機制獲得解決，因為目前國際上主要國家，均有專法針對網際網路垃圾郵件問題予以規範。

有鑑於此，國家通訊傳播委員會（NCC）於 2007 年 12 月底，發布新聞稿對外界說明我國對於垃圾郵件氾濫議題管制的立法進程，以行政院於 2005 年提出的「濫發商業電子郵件管理條例」草案為基礎，並參考立法院科技及資訊委員會審議中的四個相關法案，經綜合研析，草擬完成新版「濫發商業電子郵件管理條例」之建議法案，未來將依規定完成法制作業程序後送請立法院審議[13]。

第三項 憲法框架下的觀察

國家選擇以立法途徑介入、管理網路垃圾郵件氾濫之問題，確有其必要性，且合乎國際潮流，值得吾人為其喝采。惟若從憲法之角度觀察，任何涉及憲法所保障人民基本權利之侵害，除應有法律

[12] 例如中華電信股份有限公司網際資訊網路業務(HiNet)租用契約條款第 46 條，乙方(網路使用者)有下列情形之一者，甲方有權暫停或終止乙方於甲方 Internet 服務之所有帳號或終止甲方 Internet 服務之所有契約，並由乙方負一切法律責任；且於停權期間未滿時，拒絕提供乙方所有 Internet 服務：「……6.濫發電子郵件、蓄意破壞他人信箱或其通信設備之情事者。……」

[13] 國家通訊傳播委員會 2007 年 12 月 25 日新聞稿。

依據外，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理、正當，方符憲法保障人民基本權利之意旨。

因此，應當要探討的是管制垃圾郵件之法律規範，其採取的管制手段是否能夠合乎各種憲法原則的要求？是否對於某種基本權利進行過度的限制而無法通過比例原則檢視？從基本權利的積極面向來看，國家的立法對於受到侵害基本權利是否能充分保障？目前世界各國大部分的立法，大多將打擊面限縮在商業電子郵件，主要的考量除了目前以推銷商品為內容的電子郵件數量最多之外（約占整體垃圾郵件總量的 30%），另一個主要顧慮即是在於為了避免逾越憲法保障基本權利的界線。

第二節 文獻回顧

環顧國內專書文獻對於網際網路垃圾郵件法制之研究，主要的關懷集中在外國法制的譯介，以期作為我國立法之參考。研究最為詳盡者首推國家通訊傳播委員會編著，於 2008 年出版之《濫發商業電子郵件防制監理機制研究[14]》一書，該研究報告共分為五章：

第一章 緒論

第二章 各國防制濫發商業電子郵件規範之比較

第三章 行政院版本與各立法委員版本之比較

第四章 本會監理機制之規劃

第五章 結論

該研究報告除了參研各國電子郵件管理法規、立法院審議中相關管理法案外，同時亦蒐集多種電子郵件濫發手法暨防制機制；此外，亦在立法管理層面，分析探討我國商業電子郵件管理所需之立法規制方向，並就監理需求提出明確立法建議，為目前國內探討濫發商業電子郵件內容最新且最為重要之文獻之一。

另一重要文獻為行政院經濟建設委員會委託太穎國際法律事務所辦理，於 2003 年 12 月完成之《濫發電子郵件行為之管理與法制規範研究[15]》期末報告，共分為五章：

[14]國家通訊傳播委員會編著，《濫發商業電子郵件防制監理機制研究》，國家通訊傳播委員會自行出版，初版，2008 年 3 月。

[15] 《濫發電子郵件行爲之管理與法制規範研究》，行政院經濟建設委會委託太穎

第一章 研究背景與問題提出

第二章 濫發電子郵件行為的管制機制

第三章 國際管制濫發電子郵件之規範研究

第四章 我國管制濫發電子郵件行為相關規範之檢討

第五章 結論與建議

該份報告除就國際間對於濫發電子郵件管制之法制予以說明外，其主要特色在於利用面訪、電話討論及電子郵件聯繫，直接向各網際網路服務立法先進國之立法者、執法者、專家學者與反制濫發電子郵件組織的領導人進行接觸，取得第一手關於各國立法管制濫發電子郵件實踐的經驗。雖屬 2003 年之文獻，在網路科技變動快速與立法變遷等因素影響下，有部分內容已不合時宜，與現狀脫勾，惟涉及基本面論述（如思考脈絡、涉及之相關法律問題討論等）的部分，仍具有一定參考價值。

期刊論文方面，單純為外國立法內容介紹與事後賠償機制簡介者，已累積有一定數量，討論層次較為深入者，早期之文章討論以王郁琦、陳炳全，〈濫發網際網路廣告信相關法律問題之研究[16]〉為代表，較近期之文章則為黃立、蔡欣惠，〈從美國聯邦貿易委員會研究報告看「未經邀約的商業電子郵件」標示主旨欄之必要性[17]〉。

學位論文方面，大致上追隨期刊論文的腳步，以外國法制介紹比

國際法律事務所辦理期末報告，2003 年 12 月 31 日。

[16]王郁琦、陳炳全，〈濫發網際網路廣告信相關法律問題之研究〉，《月旦法學雜誌》，2002 年 2 月，頁 152-166。

[17]黃立、蔡欣惠，〈從美國聯邦貿易委員會研究報告看「未經邀約的商業電子郵件」標示主旨欄之必要性 〉，《律師雜誌》，第 311 期，2005 年 8 月。

較與事後損害賠償機制為主[18]。唯一從憲法觀點探討者，僅有 2006 年由徐碩延撰,《從憲法基本權之觀點論對未經邀約電子郵件之管制規範[19]》，國立台北大學法研所之碩士論文。該論文討論內容打擊面相當廣泛，將各種預想中可能受到管制影響之基本權利均予以囊括並簡單論述。

由此可知，國內法律學門研究垃圾郵件管制之焦點，主要集中於外國立法介紹以及對於 ISP 業者、收信者對發信者的「事後賠償請求權」、「團體訴訟救濟」等民事法範疇；從最上位的憲法視野，來觀察網際網路垃圾郵件管制規範之文獻顯然較為缺乏，或有論及但並未著墨太多，同時進行立法政策與人權保障雙主題式的觀察之專論，似乎並不多見。

[18] 國內與未經邀約商業電子郵件管制法律議題有關的論文計有：徐碩延,《從憲法基本權之觀點論對未經邀約電子郵件之管制規範》,國立台北大學法研所碩士論文，2006 年。蔡欣惠,《數位時代下垃圾訊息法制之建置-以美國法爲藍本》,國立政治大學法研所碩士論文，2006 年。施懿玲,《垃圾郵件的侵權行爲民事責任》,東吳大學法研所碩士論文，2005 年。黃偉陵,《網路垃圾電子郵件濫發之法律問題研究》,國立中正大學犯罪防治研究所碩士論文，2003 年。其他從科技角度、軟體設計等角度探討者共計約達六十餘本。

[19] 徐碩延,《從憲法基本權之觀點論對未經邀約電子郵件之管制規範》,國立台北大學法研所碩士論文，2006 年。

第三節 研究方法

本論文預計採行下列研究方法：

一、 文獻探討法

資料彙整與研析為本論文重點之一。除既有專書、期刊之外，自網際網路上所取得之相關資料亦扮演吃重角色，理由在於網路無遠弗屆，且內容更新速度較期刊更為迅速，許多國內不易取得之資料，例如國外管理濫發垃圾郵件主管單位有關資訊，均可於網際網路中獲得。

本論文進行資料蒐集整理，主要包含國際研究與國內研究兩個面向。就國際研究，蒐集美國、日本、歐盟及所屬國家等立法例進行蒐集外，並嘗試作比較分析，並盡可能閱讀英文、日文文獻。國內研究方面，則以國內現有中文文獻與立法資料進行閱讀蒐集。

二、 比較分析法

鑑於以立法方式管制網際網路垃圾郵件已成為國際趨勢，且國內文獻資料有限，故不能閉門造車，與世界脫軌。因此有必要就國際上主要國家之立法例進行比較與分析，並將各國規範所共同採取之措施以及各具特色之立法予以歸納，作為我國之參考。

三、 案件分析法

案件分析法（case analysis），係指於進行外國法制研究時，涉及相關之重要案例，必須採取案例分析，包括事實、程序、案件中爭議與法院判決結果、論證等。

第四節 研究架構

本論文之論述架構可略分為「比較法論」以及「人權保障論」二大部分，分述如下：

第一部分為第二章〈各國濫發商業電子郵件法制〉，鳥瞰國內外有關管制濫發商業電子郵件的法規範，屬於比較法論。因各國立法目的、規範對象、處罰手段以及實施成效均有所不同；而他山之石，足以為錯，藉著比較觀察各國立法，並作為我國立法參考借鏡，故確有研究之價值與必要。又雖然國內探討國外立法例之文獻，已累積有一定數量，為避免研究重複，本不應再闢專章說明，惟基於以下原因考量，仍以一章的分量討論之：

一、 完整性：

由於濫發商業電子郵件法制，究屬特別立法，一般人對其之接觸機會，並不若行政法、民法等基礎法律多。再者，本論文討論重心之一，係以憲法基本人權保障的觀點就濫發商業電子郵件法制進行探討，因此，基於完整性考量，就相關法制仍應有為前提性與基礎性介紹的必要。是以，本章原則上僅作一鳥瞰式之介紹，而不為深入分析，僅為扼要整理。有關各國立法詳細的說明，敬請參閱註釋中所列之參考文獻。

二、 即時性：

於本論文寫作同時，日本正著手修訂「特定電子郵件適正發送法」，目前正由總務省進行「迷惑メールへの対応の在り方に関する研究会」，自平成十九年（2007 年）7 月 24 日起召開為期一年，預

計在平成二十年（2008 年）8 月結束，並將提出供該國法律修正參考之一系列豐富立法實證研究與報告為資訊公開[20]。相關資料目前未見國內討論，且基於參考國際濫發商業電子郵件立法，需要不斷地與時俱進，掌握修法脈動，而有即時更新之必要。因此本章就日本的立法，將作較為深入的分析。

三、 差異性

與國內既有文獻相較，雖屬相同議題，然隨著觀察角度與閱讀文獻之出入，整理歸納之方向與見解，容有差異。因此，於各節中所提出之整理方向與最後提出之歸納，與其他文獻之觀點或有不同。

第二部分則從憲法的觀點，特別是基本權利的保障出發，分別為第三章〈商業言論自由的觀點〉、第四章〈秘密通訊自由的觀點〉與第五章〈隱私權的觀點〉。國家立法管制濫發商業電子郵件所涉及的基本權利態樣，可謂相當廣泛。概括而言，舉凡言論自由、營業自由、秘密通訊自由、工作權、隱私權與財產權……等，均與該法制有所關聯。本文囿於自身研究能力有限，無法面面俱到地從各種基本權利之觀點進行論述；因此，本文欲將研究範圍限縮在較具有爭議性的商業言論自由、秘密通訊自由與隱私權三種觀點，對濫發商業電子郵件法制進行觀察與檢討，至於其他基本權利的觀點，則不在本文研究範圍之內。

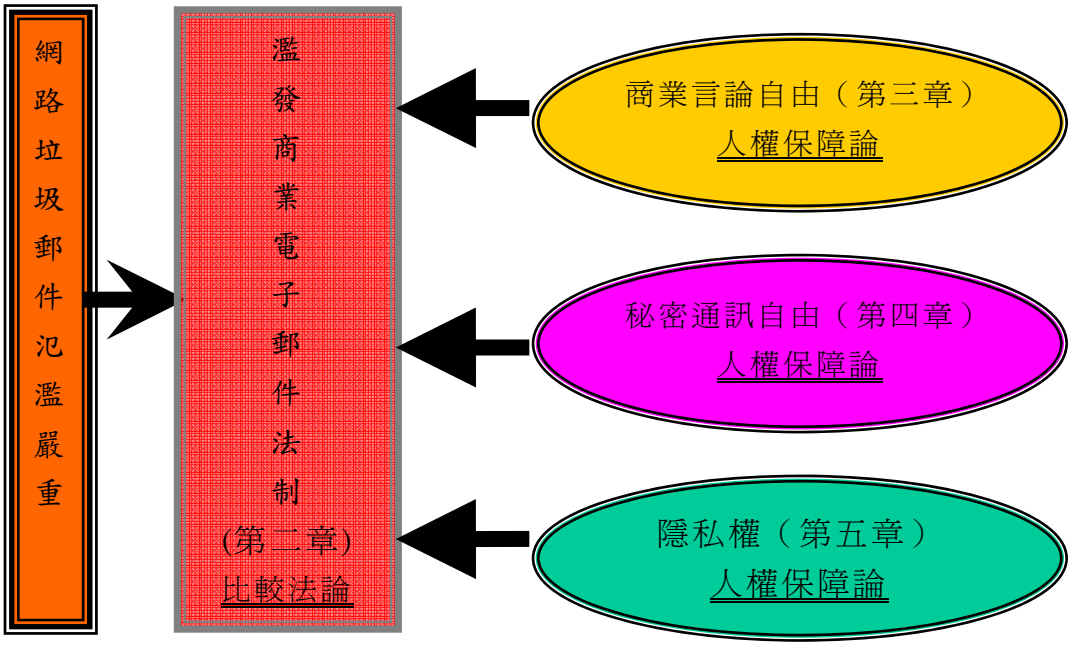
就商業言論自由的觀點而言，將首先探究商業言論自由的意涵與憲法上的發展比較，再分別就美國法制與我國法制探討相關濫發

[20]迷惑メールへの対応の在り方に関する研究会
http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/mail_ken/index.html

商業電子郵件法制是否對於發信者的商業言論自由形成過度的限制。就秘密通訊自由的觀點而言，除了將說明秘密通訊自由在通訊服務自由化的時代，在憲法上具有的時代意義之外，亦將討論濫發商業電子郵件法制當中可能涉及干涉人民秘密通訊自由的制度與通訊服務提供業者攔截阻擋商業電子郵件的手法對秘密通訊自由的影響，另並試就我國立法參考最多的日本法制進行比較與分析。就隱私權的觀點而言，除了說明隱私權在憲法上的意義外，將討論重心置於在濫發商業電子郵件的行為對於收信者隱私權侵害的態樣，是否已能藉由現行的法制找到保障依據，另外則是討論我國濫發商業電子郵件法制對於隱私權的保障是否充分；最後則是嘗試就論者提出的商業電子郵件法制規範對於發信者的「網路匿名」侵害的見解，進行評論。

最後，則以第六章作為結論，提出研究發現以及對我國規範之建議與未來展望。

本文研究架構，得以下列圖示表達之：


網路垃圾郵件氾濫嚴重
濫發商業電子郵件法制
(第二章)
比較法論
商業言論自由（第三章）
人權保障論
秘密通訊自由（第四章）
人權保障論
隱私權（第五章）
人權保障論