資訊社會研究(8)
頁 213-242，2005 年 1 月

以存取控制模式分析垃圾郵件管制之問題與對策[1]

林孟芃
政治大學公共行政研究所
simone0814@dgt.gov.tw

摘　要

即便是在近年國際立法規範趨勢與技術過濾之雙重圍堵下，垃圾郵件氾濫問題仍未見和緩之跡象。本文以為垃圾郵件之管制，不僅涉及如何將其外溢效果問題，其本質上亦與網際網路規範建構與執行議題相涉。因此有必要對電子郵件發送之規範、技術與經濟面作全盤性剖析，始得以釐清垃圾郵件問題之規範困境。

藉由存取控制模式，本文分析垃圾郵件管制策略與處理之規範困境後，認為由於訊息傳遞過程三方皆有資訊不足，加以訊息交換過程成本負擔失衡等因素，使得傳統規範與單一管制策略之採用，產生無效率之情形。基於管制目的在於消除市場失靈與資源使用的無效率，管制行為也應避免產生社會無謂損失。故本文認為，在現今的網路結構下，要能有效處理垃圾郵件問題，宜採取混合型策略。在規範設計上，也建議朝向以市場機制途徑為主，而強化對於發訊端與中介端行為調適誘因之建立。

關鍵字：存取控制模式、垃圾郵件、外溢效果、網際網路規範建構

[收稿]2004/09/09;　[接受刊登]2004/11/23

---

[1] 於此感謝兩位匿名審稿人所提供之修改意見與指正。此外，本文部分資料，得任職通訊傳播委員會籌備處法制組期間工作同仁與長官之協助，於此一併表示誠摯之謝意。惟文中觀點，僅代表個人意見。一切文責亦由作者自負。

壹 引言：垃圾郵件問題之過去與現在

今年二月，歐盟執委會委員 Erkki Liikanen 在 OECD 反制垃圾郵件的會議上指出，目前全球電子郵件中，垃圾郵件的比例已從三年前的 7%升高至目前的 58%。[2]近次的本土調查亦顯示，垃圾郵件問題除了有更加惡化之趨勢外，更將造成台灣每年耗損近六百億元的社會成本。[3]

垃圾郵件（spam）所以再度成爲公共政策上的議題，當然不僅僅在於其影響資訊傳播科技使用者，更由於其外溢效果成爲資訊科技應用與建設上的沈重負擔，而備受關注。當代傳播型態受資訊科技的影響甚深，並呈現持續變遷的風貌。許多傳統媒介規範目標與原則，如言論自由、平等近用、資訊品質或內容多元等，仍持續受到重視，但在高度技術主導性的網際網路上，由於後者有不透明性、去中心化、去中介化等特質[4]，致使垃圾郵件管制模式之選擇，將引發更爲複雜之網路社會規範模式的爭議。然而，除了科技因素外，在經濟層面上，網際網路傳播之成本低廉、外部性[5]，以及規範面上的管轄問題等，

---

[2] Erkki Liikanen, “Opening Remarks at the OECD workshop on spam,” OECD Workshop on Spam (2nd February, 2004, Brussels), available at http://www.oecd.org/dataoecd/4/43/28766599.pdf。而九月初 OECD 於漢城所召開的第二次反制垃圾郵件之工作會議中，也再次強調此一問題惡化的趨勢（OECD, 2004b）。

[3] 根據「台北市消費者電子商務協會」於今年 4 月 21 日到 5 月 3 日的網路民調顯示，受訪網友每天平均收到的電子廣告郵件，自前年的 8 封增爲目前 42.2 封；有超過八成使用者表示不堪其擾；有九成的受訪者認爲個人隱私受到侵犯，且耗費太多時間處理垃圾郵件。此外，約八成五的人認爲接受電子廣告郵件會增加額外的上網成本，高達九成五的人表示造成信箱爆滿的原因是因電子廣告郵件氾濫所致。資料來源：台北市消費者電子商務協會於陳建銘委員召開之立法院記者會上之報告，2004/06/23。

[4] 劉靜怡譯，Lawrence Lessig 原著，《網路自由與法律》，初版（台北：商周，2002 年）；See also Tal Z. Zarsky (2004: 993)

[5] 就外部性的討論，以宏觀的角度來看，網際網路之訊息流動或交換，由於減少了一般被認爲會導致市場失靈的資訊不對稱問題，故認爲帶給整體市場之淨效

均使得傳統的規範思維、架構及策略，產生管制失靈與規範落差等現象。

然而，在管制垃圾郵件問題上，我們首先遇到問題定性的困難。一般處理管制議題時，「問題的釐清」、「管制必要性及目的」、「管制策略及工具之比較與選擇」、「管制成本」、「管制影響分析：主要效果與次要效果」等要素之檢討，實不可或缺。從過往諸多國內外研究，我們清楚地肯定了此一問題管制之必要性—除了一般認爲有侵犯隱私之虞外，更同時涉及廣告不實、詐欺、色情資訊、網路頻寬之佔用、不當轉嫁使用成本，並破壞電子商務消費者的信心等負面影響。也因此研究者多頗爲一致地得出政府應立法干預之結論或建言。但對於政府應如何干預或管制，如管制對象與範圍、管制者的選擇、行爲準則之建立、甚至制裁機制等—單純以定義何爲「垃圾郵件」爲例，在學界討論[6]與各國立法例上（可參閱如附錄所示），都存在著不小的差距與爭議，此預告著未來國際合作上的困難。

藉由存取控制模式之分析，本文期待由網際網路電子郵件之訊息傳播型態切入，並探討既有的管制困境，並說明管制點選擇之理由。過往對於垃圾郵件問題相關之研究與討論，多是由既存法規範的角度切入—或討論既有法令對於垃圾郵件問題之規範漏洞（如王郁琦、陳炳全，2002），或介紹國際上的規範趨勢與評述（如陳思廷等，2004）。前述觀點固甚爲重要，但卻未能充分掌握垃圾郵件問題橫跨科技、傳播、經濟面之全貌，更罔論比較不同管制手段之差異以有助於管制策略的形成。由於管制環境與規範之間是一種動態的交互影響關係，本文以爲要分析垃圾郵件管制問題與處理前述爭議（例如何爲「垃圾郵件」？採 opt-in/opt-out 規則等問題），除了需對當前網際網路電子郵

用應該爲正值。然而目前此種與商業交易有關訊息的氾濫，卻使得負外部效果劇增。但從個體的角度來說，每封垃圾郵件之發送都有微弱負外部性產生。

[6] See e.g. David E. Sorkin (2001), *Technical and Legal Approach to Unsolicited Electronic Mail*, pp.327-336.

件之傳輸結構有充分之瞭解外，也應回歸電子郵件訊息交換本質來檢討。正由於對於垃圾郵件問題定性之差異，對於因此所界定要封阻的訊息交換，將會有管制策略與方法上的不同。對此，本文也針對目前國際規範共識上所定義的垃圾郵件，即不請自來的廣告電子郵件，以存取控制模式之分析，來討論既有管制策略之優劣。同時，本文也將提出較爲可行的做法，以確保未來網際網路之訊息流通與交換上，能維持其開放與自由之特質，並平衡電子郵件使用者、網際網路服務業者，及合法電子行銷業者之權益。

以下，本文首先說明存取控制模式之內涵與分析方法；其次，本文將運用存取控制模式於解構垃圾郵件之問題，並探討不同管制點下之規範可行性；再者，本文以現階段所定義下的垃圾郵件問題爲前提，具體討論目前既有管制策略，包括直接立法、自我管制、科技解決及市場機制等模式進行分析與檢討。最後，先歸納本文對於垃圾郵件存取控制分析之結果，並提出本文建議之以價制量且強化收訊端控制與課予中介端及發訊端責任爲主軸的市場機制策略，並輔以必要技術解決方案和管制強度較低的立法建議與理由。

貳 存取控制模式

本文是以 Lessig & Resnick（1999）所提出的「存取控制模式」作爲討論網際網路上垃圾郵件所引發的管制問題之基礎。

所謂「存取控制」（access control）是科技法學者 Lawrence Lessig 等所用以取代傳統言論檢查（censorship）而意涵更爲廣泛之概念。透過具體化存取控制的要素，Lessig 與 Resnick 將之發展成可以處理網際網路內容規範議題之分析方法，特別是被作者運用在美國著名的「網路通訊端正法」（Communication Decency Act）及其後「兒童線上保護法」（Child Online Protect Act；別稱 CDA II）規範可行性之

討論上[7]。由於傳統討論網際網路上的內容規範議題時，其類型化與管制之討論，都簡化而且預設了管轄的單一性[8]，致使管制成效不彰。然而，Lessig & Resnick 所提出之存取控制分析，其主要的特點即在於能夠處理網際網絡跨國界特質下的內容規範問題。

在處理管制網際網路上垃圾郵件流竄之問題時，也有相似的困境。首先，若以傳統管制策略與強度來面對網際網路世界中的垃圾訊息時，會由於隨著實體世界管轄權的變動，而使得該訊息是否「應」且「能」受到管制，產生重大的變化[9]。其次，雖然不少人並不認爲垃圾郵件管制與言論管制相關，但若以訊息傳播角度來理解「垃圾郵件」，根本上其實是指一種在網際網路上應受封阻而未被封阻的訊息；特別是由發信人與收信人的角度理解，應該是一種「質」的問題。然而，目前實務上特別強調的垃圾郵件問題，很大一部分是以中介端（即網際網路服務提供者[10]）的角度詮釋之結果，故而雜揉了濫發行爲（「量」）之問題。濫發行爲可以理解爲由於這類訊息傳遞中，由

---

[7] 簡言之，Lessig＆Resnick 希望透過存取控制分析美國兒童線上保護法，在不悖於 Reno v. ACLU（1997）一案之憲法見解下，期待描繪出一個近乎「理念型」的「網路內容端正法（decency act）」。兩位學者認爲此一分析方法是脫胎於於敏感性分析（sensitivity analysis）。See Lawrence Lessig and Paul Resnick (1999), *Zoning Speech on the Internet: A Legal and Technical Model*, p.395. 其後如 Nyberg（2004: 681）、Reimann（2003）或 Watt（2003）等學者討論關於平衡網路資訊流通自由及不當內容與活動之管制時，都肯定了 Lessig＆Resnick 之分析結果與管制選擇建議，也認爲存取控制能夠相當精緻地分析涉及網路內容管制之困境，其對於管制策略之建議，能使管制者免於陷入管轄衝突與內容管制敏感性等泥沼。

[8] 同上引書，作者將無法處理管轄衝突問題的傳統網際網路內容管制，稱爲“ mandatory access control”。

[9] 例如一封不請自來的色情網站連結之電子郵件，在美國、澳洲、加拿大之發信者（可參閱附錄之比較），顯然將受到不同程度之對待。又如果在未來對於垃圾郵件之定義，跨出商業（廣告）電子郵件範疇，更將凸顯此一問題跨越管轄權間的管制困境。

[10] 在垃圾郵件氾濫問題上，一般認爲將受此問題影響之網際網路服務業者，主要是指網際網路接取服務提供者（IAP）與網際網路平台服務提供者（IPP）。也正由於這些業者深受其苦，從而在其組織性的運作下，無論是國內外，都是根本上垃圾郵件問題所以備受關注與立法之主因。

於摻雜了經濟性動機或傳輸工具的濫用，致使收訊端或第三方深受其害之情形，此亦即一般所稱垃圾郵件的外溢效果（特別是負外部性的主要根源）。從而也模糊了垃圾郵件問題實爲網際網路內容管制一環之本質。再者，由於對於訊息流通或交換要進行控制，必須要能確知發訊方與收訊端之身分、管轄、及所爭議的訊息類型。而網際網路之訊息傳遞及電子郵件傳輸結構之設計與發展歷程，卻使得前述三種資訊都不易獲得確認，故產生了究竟何方應負有封阻該類訊息責任、或何方較有能力之爭議。

承上所述，本文認爲援用存取控制模式之分析方法，將有助於瞭解垃圾郵件之管制與規範議題—特別是由於未來管制範圍的擴張可能性、管制點與懲處機制之選擇等爭議上，除了一般規範論必然考慮的公平因素外，更應有合乎經濟成本與效率之思考。畢竟，垃圾郵件之管制將是在法律與網路結構[11]下產生其影響；事實上，網路法律必然是須在網際網路結構之架構下發揮其作用的。

也因此，爲充分瞭解管制垃圾郵件之問題，以下將簡要介紹此一分析架構之內涵，並將在下一個繼續檢討在電子郵件訊息管制之議題上，不同法律規範與網路結構選擇之設想情形。

一、基本分析單元及傳播型態

網際網路傳播的基本組成單元，我們可將之簡化爲發訊端、收訊端、及中介端來討論[12]。本文將假定在網際網路傳播過程中，此三方對於受管制之內容有不同程度的瞭解。基本上，發訊端假定爲可以完

[11] 此處所稱的網路結構，實包括了有網際網路技術協定（protocols）、所採用的標準（例如數位認證系統、瀏覽器）以及被管理者或使用者所強化的習慣。這些網路結構並非是固定不可變動的，與實體法律的關係，應該說是一種相互影響的過程。

[12] 因爲即便是在最簡單的郵件傳遞過程中，也至少是發訊端（若又假定其爲自架電子郵件伺服器者）、網際網路接取服務業者（存取伺服器）、及收訊端。不過，在通常的電子郵件傳遞過程中，中介端經常是複數。

全確知其所發送的內容；收訊端是被假定徹底瞭解自身的特質（如年齡、是否已經預先同意接收該訊息）與所在地管轄（Lessig &Resnick, 1999: 399）。

然而，與原模式不同的是，本文並不特別預設中介端對傳輸內容或收訊端的身分特質或所在地一無所知之前提。因爲在垃圾郵件問題中，存在一種並不少見的情形，就是電子郵件服務提供者本身即爲訊息發送者，且透過註冊資訊瞭解其服務使用者之資訊。 本文以爲，除了瞭解靜態的組成單元外，電子郵件的傳播型態也應納入考量因素。網際網路傳播型態十分多樣，並且持續演變中；對於不同的傳播型態，傳統上也發展出相對應之管制架構[13]—雖在網際網路上無法移植，但其所據理論與所受限制，亦足茲從事規範建構之參考。

除上所述，本文中之「存取控制」之分析，另包括：第一步，必須明確定義出不合法的訊息傳遞之類型；其次則爲管制點之選擇，即指課予其中一方或多方責任以達成限制或控制其行爲之效果；再者，此一控制也同時也應設計出一可執行之機制，使得前述義務之違反得以追溯，並且考慮管制成本因素。此外，本文也會如原作者一般，論及相關管制措施可能產生之正面效益與副作用。

二、界定所欲封阻之訊息傳遞

[13] 如 McQuail＆Windahl 就將典型的訊息傳播模式分成三類：「廣播型」係指利用無線電波傳遞訊息的傳播媒體，包括廣播與電視等，其特點在於具有閱聽人不必向發訊方請求即可自行收訊之特性；「印刷型」則指報紙、雜誌等媒體，其具有閱聽人必須向發訊方請求（例如訂購）才能閱聽之特性。以上兩者皆屬於一對多的傳播型態；「共通載具型」則是泛指一般人際間（點對點）的互動型溝通方式。從歷史的角度看其區分的實益，在於其實質上的管制理由與強度有異。詳可參閱如 McQuail, Denis and Sven Windahl (1993), *Communication models: for the study of mass communications*, pp.205-211. 而事實上網際網路之傳播型態係雜揉了上述多重訊息傳播模式。

首先，決定是否爲所封阻或制止之訊息傳遞（B），其主要因素有：「資訊類型」（I）、「收訊端之類型」（R）、以及「管轄」（J）。據此，Lessig 與 Resnick 提出如下之關係（Lessig & Resnick, 1999: 399）：

B（I, R, J） ＝ <lcub> Y, N <rcub>

易言之，假使該訊息傳遞是被封阻或制止，則該公式之結果爲是（Y），反之則爲（N）。

又如以不合法資訊交換爲例，將可能是係基於特定類型訊息之存取，如行銷資訊（*m*）；又收訊端已拒絕（*d*）；又在特定管轄權內，該行爲管轄地之法律所禁止或不禁止等因素所決定。其關係及所得結果如下：

B （I*m*, R*d*, J） ＝ N

針對資訊類型部分，首先我們將遭遇何謂垃圾郵件之定義困擾—這一點也成爲立法管制之主要原因。在缺乏對於垃圾郵件定義的共識下，最廣義來說，所有收訊端所不欲接受的訊息，都可以歸類成垃圾郵件。然而此種定義正好使得收訊端成爲訊息傳遞過程中，封阻效率最高（大概也是目前的情形，但卻帶來其他的副作用）；反之，當垃圾郵件之定義或標準越明確化，基於發訊方最充分瞭解訊息的內容，因此其封阻能力也就越高。而中介端的封阻能力，則是依訊息的標準化程度而異。

此外，特別要注意的是管轄因素。由於網際網路此一傳輸平台無遠弗屆的穿透力及特質，致使網際網路規範議題尤爲複雜。在垃圾郵件問題中，同樣的訊息類型或收訊端因素，但因管轄之不同，而將有不同的結果。討論管轄之前提，事實上也在於有明示之規則（特別是所禁止傳遞之訊息類型）—不過並不預設該標準究竟是由行政或司法機關，或甚至是獨立的第三方爲之。

三、責任配置與管制點之選擇

任何管制策略的選擇，都將產出不預期的結果與行動。在此分析步驟中，是意圖在前述訊息傳遞過程中，找出最佳的管制點或責任配置型態，以利其後可兼顧技術、效率與規範公平性等因素來考慮相關之管制策略。首先，就管制點的選擇問題，此一決定可說是以外力去平衡原本訊息傳播關係中控制力不對稱之基礎結構與利益成本分配，其與未來規範上之責任分配有相當程度的連動關係。舉例而言，若如一般所定義垃圾郵件爲大量未經邀約的廣告郵件，則很明顯的直接利得是在發訊方，成本負擔則集中在中介端及收訊端身上。不過中介端有能力透過價格機制來將其成本轉移到發訊方或收訊端，收訊端只有在受到明確的損害時，才能夠透過計有的損害賠償體系來轉移成本。至於在訊息控制能力，則發訊方高於中介端及收訊端，因此若考慮此一因素，則管制點選擇在發訊方則較有效率。

此外，法律基本上就是一套以產權制度與責任體系來創造行爲誘因之制度。第一步係透過產權，宣稱誰擁有何權利（Lessig, 1999: 519）。藉此，而得創造一方或多方有停止或封阻該資訊傳遞之誘因。常見兩種責任規則與責任分配方式[14]於影響行爲結果上，將有著重大差異。「原則禁止，例外許可」是必須在法律顯示其行爲合法之前提下，才能免除其責任—傾向於預先防範。「原則許可，例外禁止」則是在事後被確定是違法時，始加予一定之罰責—以一般過失責任型態來評價。至於責任分配方式也可以透過比較效率與公平等，而獲得較佳之方案，不過其複雜性非本文篇幅所能處理，暫時加以省略不論。

四、監督與執行

不過考慮到垃圾郵件跨越科技、經濟、隱私權等層面之複雜性，本文在其後之運用上並將更進一步導入成本因素之考量。

[14] 一般而言，概可有四種選擇：「有能力者承擔」、「獲利者承擔」、「引發風險行爲者承擔」、及「共同分擔」之責任方配方式

爲達成管制之目的，管制者必然須構想出有效率、合憲且可行之策略。特別在網際網路的問題中，各種類型管制措施之使用深深地影響整個存取控制之監測成本。此外，無論是以行政或司法機制的干預，或採自我管制等策略，是否能夠有效率地達成管制目標，而不至於耗費社會成本過劇。誠如管制環境污染一般，從成本的角度來說，如果總管制成本還大於被管制行爲所造成之社會整體損失，那麼該管制行動將因不具經濟效率而欠缺正當性。

參 垃圾郵件管制議題之綜合分析

一、電子郵件之訊息傳播模式

電子郵件之傳播模式，不同於最常見的網路訊息傳播型態[15]。前者並非預設爲端對端通話層的傳輸模式，而是一種遵行 TCP/IP 的網路通信協定，如 SMTP（port 25）或 POP3（port 110）之結構。易言之，電子郵件之訊息交換條件，僅關注正確的收信位址，至於內容及發送位址並未有實質要求。在確知位址的前提下，電子郵件使用者皆可以主動的發佈訊息給他人。然而，在訊息承載空間有限的情況下，雖然理論上每個收訊有自主性的選擇是否去接觸該訊息之可能，但卻可能因訊息過載而因此排擠掉其他可能傳遞而來的訊息。又相對於技術結構上，所允許發訊端自由的表意能力而言，收訊端在訊息過濾的能力上，與廣電媒介使用情形相似，只有在初步接觸後，才具有過濾或回應之能力。這使得當前電子郵件的訊息傳播模式，實際上是一種接近廣電類型之單向傳播模式。

此一科技層面的結構性因素造成幾種結果：其一，電子郵件發訊端，在缺乏其他行爲誘因的情況下，更無獲取關於收訊端及管轄等相

[15] 本文指的是全球資訊網（World Wide Web）之訊息傳遞模式。其特點在於接收訊息者往往是主動點選該資訊後，才會接觸資訊，並非總是暴露在不預期的訊息中，故與傳統媒體，特別是廣播電視有所不同。

關資訊之動機，惡化其原先資訊不足的情況，即如使用位址蒐集軟體、或使用字典式攻擊法等來大量發送電子郵件。其次，由於網際網路與電子郵件傳輸型態之可匿名性特質，致使收訊端只有消極的訊息拒絕權力，而處在一種不完整的表意自由中。

是故，可知發訊端與收訊端在資訊自主權上，顯然處於控制力失衡之情形；然而傳統依訊息傳播模式而異其管制強度與控制點之管制架構，在此時卻已難再適用。

二、界定所欲封阻之垃圾郵件

首先，以一般所謂的垃圾郵件來說，發訊端對於訊息內容之認知程度，是資訊最充分者，且可事前獲知。但從另一方面而言，在沒有外力介入強制定義下，收訊端基本上才是最終決定該電子郵件是否爲其所不欲之訊息（unwanted message）。故兩者在規範定義明確具體與否下，其所掌握資訊充分性之先後次序，即有不同。以一般普遍對於垃圾郵件之定義「未經邀約、大量、廣告」來說，這實即是以第三方（管制者）強力介入個人資訊自主權。畢竟，即便符合上述定義，也無法一概否認此類訊息皆爲所有收訊端所拒絕讀取之可能。

其次，就收訊端之類型來說，一般而言，中介端要比發訊端更有能力彌補資訊不足之情形，例如透過註冊使用時，從事個人資料或收訊意願之調查。而發訊端則可能可以在電子郵件位址蒐集的過程中，蒐集到此類資訊。但在目前電子郵件發送技術之下，若無其他外力干預，發訊端並無行爲誘因去辨別收訊端特性。

最後，由於網際網路有跨國界之特質，故在管轄方面則顯得格外複雜。因爲發訊方無法確知收訊端所在管轄地之管制情形。再以現況爲例，國際間目前並非皆對於垃圾郵件有所規範，已規範國家間標準也未盡一致—此導致兩種結果，其一，即便是相同的電子郵件內容，發訊方也可能因爲不可預知管轄，而遭來不可預見且不同之違犯效

果。其次，由於管轄差異，發訊端可遁入對垃圾郵件「友善」之區域來對外或對內發送電子郵件。此顯示管轄議題與國際規範差異在反制垃圾郵件行動上之關鍵地位，也所以格外凸顯國際合作之重要性。

三、責任配置、管制點及管制成本

首先，針對管制垃圾郵件議題之責任規則選定一事分析，從訊息傳播所涉及之言論自由角度來說，若於內容不確定的情況下，欲採行「原則禁止法則」，將封阻過多資訊傳遞而超過國家在管制上的合法利益；然而在採取「原則許可法則」下，關於應封阻的資訊存取卻將因誘因不足而使得封阻率偏低。是故，在決定責任配置時，必須個外注意到得以降低不確定性的網路結構變動（Lessig & Resnick, 1999: 405）。然而在現階段所討論垃圾郵件管制上，多特別強調避免妨礙電子郵件使用之便利性與普及性下[16]。又以執行此兩種規則之成本而言，在垃圾郵件問題脈絡下，「原則許可法則」（選擇退出）顯然是管制成本較低的規則選擇。

其次，由於我國反制垃圾郵件之立法內容未臻明確[17]，針對不同管制點與歸責選擇之差異，以及網路結構之可能變動，本文仍有初步分析如下：

（一）發訊端責任

以目前一般認爲發送垃圾郵件之行爲成本不合理分配到中介端、收訊端身上來說，此一責任分配要求管制發訊端將發送垃圾郵件的社會成本內化，看似爲一較公平，且爲人所接受的方案。

然而，此種責任配置要求發訊端必須在發信時確定管轄規範與收訊端對象，以當前的網路電子郵件傳輸結構來看，除了對發訊端而言

[16] 可參閱如 OECD (2004a: 6) 及 OECD (2004b: 10)之討論。

[17] 目前我國「濫發商業電子郵件管理條例草案」（暫訂）預計在十一月中旬於行政院審議。

成本極爲高昂以外，確保此一責任確實執行的管制成本也可能相當驚人。

但假若此一配置確定，則爲確保管制可行性與效率，網路結構很可能將隨之變動。可能隨之發展的將是數位認證系統[18]、請勿來信登記之建置[19]、標示或電子郵資等方案。前二者意在在提供發訊端有足以辨識收訊端與管轄之資訊；後者則是相當程度地改變發送電子郵件行爲的經濟特質。

（二）收訊端責任

倘若不考慮垃圾郵件氾濫的經濟性特質，此種責任配置的方式是有著一些優點。畢竟，收訊端事實上是對於何謂垃圾訊息最有決定權之一方。又因垃圾郵件而受損害之情況難有客觀標準，收訊端責任也充分瞭解自身的訊息需求，故即便基於現行法律，也得據以主張權利。

雖然如此，但此一歸責之缺陷，卻發生在損害產生後，格外鮮明。就事後已認定爲垃圾郵件之訊息而言，收訊端所遭受之騷擾與損害，只能補償或避免損害擴大而無法恢復原狀。再者，面對網際網路上數以千百萬計的潛在發訊端，採用此責任配置之結果，正如公害問題一般，收訊端必須進一步承擔額外成本才能獲得損失賠償，但個別受害者所據以對個別加害者採取行動的誘因卻很小、甚至難以特定。又納入前述濫發行爲所致成本轉嫁問題考量，將封阻郵件之責任分配

---

[18] 惟此種認證，可以是對發訊端也可以是對收訊端要求。關於網際網路行銷方面之數位認證技術與法制議題，可參閱如 A. M. Froomkin (1996), “The Essential Role of Trusted Third Parties in Electronic Commerce,” ***Oregon Law Review***, Vol.75, pp.49-115.

[19] 不過美國聯邦貿易委員會（FTC）在今年 7 月依法向國會提出此建置規劃研究報告時，基本上前者認爲於現階段建置全國拒絕來信登記，並無助於解決垃圾郵件問題。全文請見http://www.ftc.gov/reports/dneregistry/report.pdf （最後瀏覽日期 2004 年 7 月 14 日）

給收訊端，更擴大發送垃圾郵件行爲之利益與成本分配之失衡，實無法滿足社會大眾之正義觀感。

簡言之，以目前一般人觀點與不堪其擾之態度，此歸責之低接受度，概可預期。

（三）中介端責任

此一歸責的優點，從管制者的角度看來，格外明顯。由於中介端的數量遠遠少於發訊端與收訊端，且管制對象可得特定（特別是網際網路匿名性、跨國界的特質下），因此就規範執行可行性與監督成本而言，都遠較前二種責任配置選擇爲低。中介端作爲無涉訊息偏好的第三方，其受管制的順服度，也應較發訊端高。此外，在管轄衝突問題上，也較易認定與解決。

然而，誠如前述，受限於中介端對於訊息內容屬性或收訊端等資訊不足之先天限制[20]，-而在封阻垃圾郵件訊息上產生無效率之結果。首先，網際網路上的訊息傳輸是封包型態，一般網際網路服務業者在技術與成本上無法作個別訊息之判斷，因此多是以 IP 位址來作接收端與發訊端的全面阻絕。而此將從而導致誤檔情況的大量產生。再者，發訊端要迴避此類以 IP 位址爲基礎的封阻技術，也是甚爲容易。

而此一種責任配置的採取，在網路結構上的變遷，除了前述的數位認證、電子郵資外，IP 位址資料庫建置與過濾技術之發展，將得以提升於中介端封阻與管制執行之效率。然而此類變動卻又不可避免的將與網路隱私權保障爭議糾纏不清。

---

[20] 更進一步言之，不同應用層級的網際網路服務業者對於垃圾郵件的控制能力也有所差異，可採用的控制存取控制策略也將受限。以曾經爲技術專家所提出的電子郵件側錄裝置（Mail DVR）爲例，即便不考慮此一技術的適法性問題，除非發訊端是利用網際網路平台服務業者之電子郵件收發服務，否則此一機制對於自架電子郵件伺服器的發信者，並無法執行。對於此類發訊端，具有來源處控制力的僅有網際網路接取服務業者，收訊端的存取伺服器（業者）僅能以透過判別技術來拒收整批郵件而已。

綜合以上所論，可知在垃圾郵件傳遞過程中，並不存在任何一方有充分的資訊得以進行完美的存取控制，過去強加於特定一方的強制存取控制，也因爲管轄問題與對象難以特定，而實際執行上的困難。本文以爲管制點與管制策略之選擇就必須配合各組成份子之能力、成本分配之公平性等要素作考慮；每一種配置選擇，也須進一步連帶地思考對於既有法律與網路結構的相應變動，始能有效地進行存取控制與降低管制成本。又即便該管制策略之選擇，得有效解決垃圾郵件問題，但其具體採行之技術或立法方案，也仍然必須經過更高層次的適法性檢驗。

配合前述的責任規則選定之討論，能夠補充「原則許可法則」之失以及免於強制單方進行存取控制的配套方案，就是對訊息作標示。基於標示是針對訊息類型之故，故應可課與對此資訊最爲充分之發訊端。畢竟，近來國際之共識並不希望將解決垃圾郵件之責任，加諸在一般使用者與服務提供者身上（OECD, 2004a: 3）。又如果訊息被要求標示，那麼中介端與收訊端都能更容易地判斷訊息的類型，特別是給予收訊端自主進行過濾之機會；而發訊端進行標示之成本，也遠低於個別收訊端判斷資訊內容之耗費。因此可以認爲搭配以發訊端責任之規則，始可接受。不過，完全的標示（例如未來配合網路內容分級規範所要求之標示等）與配合過濾軟體所帶來的副作用，就類似高密度的網際網路內容審查（Lessig＆Resnick, 1999: 424-426）。雖然，事實上可能不至於出現此一種極端情況，但過濾技術的發展確實可能使得收訊端減少與一些訊息接觸的機會而不自知，此向與強調資訊無障礙的網際網路內容管制政策有所相違。除此以外，此種標示規範要求也多受到支持網路經濟發展論者與行銷業者之反彈，如認爲此管制措施的一般例外條款（既有客商關係下排除標示義務）並無助於解決垃圾郵件氾濫，但卻顯然不利於小資本的商業活動發展[21]。

[21] See e.g. Joseph P. Kendrick (2003), “SUBJECT: ADV:”ANTI-SPAM Laws Force Emerging Internet Business Advertisers to Wear the Scarlet "S", p.574.

肆 既有管制策略之評析

藉由前述分析，概已能捕捉了對於管制垃圾郵件之規範內容與手段選擇之議題上之可行性。儘管既有的管制垃圾郵件方案不勝枚舉，但本文仍傾向將之歸納爲常見的四種策略類型—大致有立法規範、自我管制途徑、科技解決與市場機制等四種[22]，來進行個別檢討。

礙於篇幅，本文不擬重複過去相關研究者已有之介紹，而結合前一節之討論，而直接進入該解決方案之爭議與困境，目的在於指明採取採行該種策略必須要特別處理之問題。此外必須先加以澄清的一點是，與此前討論垃圾郵件管制之規範議題不同，以下這些方案雜揉了不同的控制點選擇。亦誠如OECD反制垃圾郵件會議之結論所言，對於垃圾郵件之管制，咸多認爲應該採用一種多元的途徑（multi-disciplinary approach），並仰賴此一訊息傳播過程中的各利害關係人通力合作，始得以成功（OECD, 2004b: 2）。易言之，下述管制策略間並無排他性，其長期或短期收效亦各異。

一、立法規範

目前國際上研議垃圾郵件解決方案之討論，多必然首先呼籲各國採取一定的法律規範，其主要是理由除與當前資訊社會下越發重視資訊安全與隱私權保障有關，大致說來，立法規範之最受推崇之一點，在以公權力爲後盾明確揭示特定電子郵件之發送規則，且得以透過程度不一的懲處機制而提高發訊端的成本，從而抑制濫發行爲。研究亦指出，法律規範的介入甚至對於其他解決方案之成效，都有一定的正面效果。[23]目前一般可知已經採取立法規範模式之國家，頗符合前述存取控制分析下之規範架構，而多傾向於選擇發訊端作爲管制點。少數例外情況（如目前加拿大反垃圾郵件法草案）則一併對中介端進行

[22] 此外，國內對此有較爲全面性討論的，可參閱如張鎮遠（2000），垃圾郵件的規範管理研究，國立臺灣大學商學研究所博士論文。

[23] 張鎮遠（2000: 251ff）。

管制（即網際網路服務提供者），並且限縮管制對象。其實際管制效果，卻差強人意[24]。

事實上，此一策略成敗之關鍵，除了前述管制規則之分析外，主要仍是在規範落差與執行面之問題上。首先，在具有規範效力的國際合作實踐前，實體世界的管轄衝突與規範差異，誠難見有效的控管。如在歐盟與澳洲等國家，在以保障個人資料與隱私爲中心，而採取較爲嚴格「選擇加入」，但美日等國則希望兼顧網路經濟發展等，而僅要求「選擇退出」規則；對於電子郵件位址之保護與垃圾郵件發送軟體之使用，規範情況也不一。即便是共識上其管制對象同爲「電子廣告郵件」，但定義是否納入數量條件、擴大到其他不請自來的電子郵件、或例外排除類型‥等[25]，都成爲處理跨國流竄的垃圾郵件之困難。

其次，關於懲處機制的設計問題，目前一般多認爲賦予網際網路服務提供者與收訊端有民事損害賠償請求權，得以以事後管制來將垃圾郵件的外部性內化，成效最佳。此外亦有是否課以刑事處罰之爭議。但無論何者，其執行之核心障礙，都在於現今網際網路電子郵件傳輸結構並不要求確實之發信位址。因此，對於政府（如果採行刑事制裁或行政裁罰）或個別受害者而言，確認發訊端身份頗爲不易、成本高昂，訴訟經常曠日廢時（Sorkin, 2001: 380-382）。前述懲處機制之差異僅在於管制成本由何者承擔。一般所寄望刑事制裁之遏阻作用，尚視未來投入執法資源與效率而定。簡言之，若在現今的網路結

[24] 目前雖然近年來先進國家都有立法規範垃圾郵件之趨勢，也有大型 ISP 業者起訴濫發者之案件，惟由垃圾郵件越趨氾濫之勢而言，立法效果顯然不彰。See e.g. Paul Jamieson (2004); Elizabeth A. Alongi (2004: 269). 事實上，從兩次 OECD 反制垃圾郵件會議之討論內涵與策略之交流，可以瞭解雖然國際間仍普遍期待立法規範，但其目的係在於作爲國際合作與協調各國 ISP 業者反垃圾郵件策略之基礎。而對於立法管制垃圾郵件成效之討論，如針對美國的 CAN-SPAM Act（15 U.S.C. §§ 7701-7713 (2003)），可另參閱如 Jacquelyn Trussell (2004), Is the CAN-SPAM Act the Answer to the Growing Problem of Spam?; “US Anti-Spam Law Fails to Bite”, BBC NEWS, Feb.9, 2004, at http://news.bbc.co.uk/2/hi/technology/3465307.stm (accessed Nov.9, 2004).

[25] 國際規範之情形，可見文末附表或參閱如經建會委託研究報告（太穎，2002）。

構下，既有懲處機制都不可避免帶給管制機關沈重之負擔，也連帶將間接降低執行上之效率。

除此以外，以管制工具之特性而言，採用直接干預型的立法規範途徑，也不免要引發對於網路內容與網際網路上活動之開放性與自由之討論，亦與目前低度管制的網際網路規範架構，不甚相稱。以前述要求標示訊息類型之管制方案爲例，雖然提高了過濾可能性且降低不明郵件所可能導致的進一步損失，但同時也降低接收到不預期訊息的可能性；過濾機制架構的越細密，對於訊息流通與交換的阻礙性也越高。雖然如 Lessig＆Resnick 等對於要求標示之作法仍懷抱疑慮，但或許高估了其風險，畢竟網際網路訊息流通管道並非僅限於電子郵件而已。

二、自我管制

此一方案在美國的脈絡下，主要是指行銷業者間及發送端之自律。由於相對於歐盟等國對垃圾郵件較嚴格之管制標準來說，美國立法體例中則創造出一得以合法發送廣告郵件之空間，故其配套方案其一，就是期望能仰賴美國行銷協會（Direct Marketing Association）之自律功能，來約束電子郵件行銷活動。此外，英國雖依循歐盟共識，雖採行「溫和型選擇加入」規則（soft-opt-in），但在行銷業者自律機制部分，也相當倚重。[26]

國際間一般也對此類自我管制策略抱持正面的看法（OECD, 2004a），但並非狹隘地僅指發訊端的自主控管。原則上此途徑是一種同時可以在發訊端、中介端與收訊端三方同時採行的途徑。特別是針對自架電子郵件伺服器的企業與個人皆應有一套電子郵件管理政策，並對其郵件伺服器作相當之管理，防止受到垃圾郵件之騷擾或成

[26] （太穎，2002: 342-344）。而有關英國相關資訊可見 http://www.cap.org.uk/（最後瀏覽日期：2004 年 7 月 7 日）或參閱「英國廣告行銷推廣與直銷規範」（British Code of Advertising, Sale Promotion and Direct Marketing）文件。

爲他人發送垃圾郵件之跳板。在網路結構之變遷上，最明顯的是一改過去有助於電子郵件發送之郵件代理伺服器與自動轉信功能等（即指防護或關閉 open proxy 及 mail relay）。

論者以爲，自我管制策略基本上無法脫離科技解決方案而運用；且若欲有較顯著的效果，也必須有一套備而不用的強制規範爲後盾。更重要的是，許多垃圾郵件雖以行銷爲名，但事實上是行詐欺或盜取信用卡資料等，如「網路詐騙郵件」（phising），根本非自我管制此一強調預防功能之途徑所可處理之範圍。

三、科技解決

簡言之，一般所以推崇科技途徑，除不受此前討論規範規則選擇之影響，大抵著眼於此一方案最具彈性與發展性。[27]責任分配之管制規則選定上，雖然或多或少會影響積極發展過濾技術之誘因，不過基於濫發行爲對於網際網路服務業者之損害以及此類資安產品的潛在市場，概可以忽略此因素之影響力。

此一解決方案主要可分成兩大作法。一般性的策略是強化中介端與收訊端積極採用垃圾郵件過濾技術，諸如 Brightmail 等反制軟體、黑名單（Real-time Black List; RBL）或白名單（white list）、貝氏過濾法（Bayesian Analysis）等過濾技術。然而，對於此種科技解決策略之評價，以目前垃圾郵件仍然氾濫之情況來看，大抵亦可見一二。主要理由，除了因爲垃圾郵件本身就是資訊科技的產物之一，因此也會隨著網際網路的發展「日益演進」外，缺乏協調的過濾工具也被認爲是可能因素[28]。此外，許多既有的垃圾郵件過濾技術也往往須受到既有規範之挑戰（例如言論自由、隱私權、服務契約等）。後兩者幾

[27] See e.g. David E. Sorkin, supra note 5, p.356; OECD (2004b).

[28] 此亦即 OECD 第二次反制垃圾郵件工作會議之討論核心之一。相關討論，可參閱自 http://www.oecd.org/document/39/0,2340,en_2649_22555297_33680935_1_1_1_1,00.html。

乎也即是許多網際網路服務業者殷切期盼立法之理由。最後，技術過濾另一種最令人詬病的缺陷，在於其不透明性與欠缺課責機制。[29]

這種科技的使用，很可能會有如 Balkin（2004）等人所質疑的，服膺於高技術能力者或業者之利益，而會有引發另一種社會衝突類型。不過也有關注於程式碼與網際網路規範的學者認爲，儘管利用科技途徑，也就是通訊協定來管制網際網路的內容，不可避免地要面對言論自由保障條款之挑戰。但其以爲以通訊協定爲核心的技術控制，仍然是目前能夠避免因爲管轄權問題（及規範落差）解決網際網路內容管制問題之良方（Nyberg, 2004: 688）。

另外一種根本的解決方式，也是爲了處理規範執行問題時，不得不面對的網路結構之改變。如將電子郵件傳輸結構改爲必須確認來源之電子郵件的傳輸協定之討論[30]，目的即在於發展能確認傳送電子郵件者與郵件上載明的發信者身分一致之郵件傳輸協定—而此正是目前簡易郵件傳輸協定（SMTP）所無法做到的功能。本文以爲若能實現此一變革，則將使得管制者執行垃圾郵件的存取控制將會有快速的邁進。也因此，結合中介端與收訊端責任之歸責與控制，將使能夠產出最大利益與負作用最小之結果。惟因此未來電子郵件要能成功傳遞門檻，也將隨之提高。

本文以爲，由於目前發送垃圾郵件的技術與反制技術間，幾乎可說是一場沒有終點的競賽，難以給予使用者完整的保護。採用技術控制策略的風險之一在於收訊端恐怕是最爲弱勢與失去控制力的一方。畢竟，以網際網路服務業者的角度來說，其念茲在茲的其實是大

---

[29] See David E. Sorkin, supra note 5, p.356; 此外，如 Lessig 之著作中（劉靜怡譯，2002），亦有類此思維。

[30] 唐慧文，〈反垃圾郵件協定邁向整合〉，CNET 新聞專區，2003 年 10 月 27 日（最後瀏覽日期：2004 年 7 月 2 日）；陳奭璁，〈垃圾郵件氾濫 SMTP 該壽終正寢？〉， CNET 新聞專區，2003 年 8 月 04 日（最後瀏覽日期：2004 年 7 月 3 日）。

量訊息發送所導致頻寬佔用與電子設備運算能力之消耗，而並不關心訊息內容與收訊端偏好之問題。因此，若未達干擾業者系統之情況下，誰發出多少帶有廣告、詐騙、色情等郵件，網際網路服務業者並無採取反制行動之誘因；而對於受過濾的訊息或被封阻的 IP 位址是否有錯誤，也往往不會是網際網路服務業者所首要關心的。因此在過濾技術的發展上，也欠缺客製化等服務發展之可能。而受到中介端主導的嚴密技術控制，又恐將將使電子郵件此種訊息流通工具，趨向於封閉，也將連帶改變未來對於電子郵件之使用習慣與信箱空間權利性質，但此已爲另一論題。

四、市場機制

從行銷型電子郵件氾濫的經濟動機—因爲網際網路行銷簡便、快速、便宜；即便郵件回覆率低，獲利仍高—來思考，則能夠一定程度地提高發信者之直接成本，不啻爲一種緩和垃圾郵件氾濫之替選方案。此外，回顧整個電子郵件服務供給市場之發展，網際網路服務業者實亦爲垃圾郵件氾濫問題之「幫兇」。

首先，爲了維持用戶數與該入口網站市佔率，大量易申請、高容量之免費電子郵件服務提供，成爲業者競逐的市場；加上胃口遭到網際網路服務業者豢養的使用者，付費使用或功能性高的電子郵件服務市場，日益萎縮。事實上，一般使用者需求有其一定之範圍，花費於電子郵件信箱管理的時間心力有限，故業者競相以信箱容量、免付費使用爲號召，卻未能致力開發更高品質之電子郵件服務，使得高品質或功能加值的付費電子郵件服務市場難以全面性開展。免費電子郵件信箱及私人架設的伺服器，都是垃圾郵件的主要發送源之一。再者，目前一般電子郵件使用者對於網路資源之價值認知欠缺，亦少有良好的郵件信箱與位址管理習慣，也通常是個人信箱中充塞垃圾郵件之原因之一。

簡言之，若以市場自願性交易爲設計基礎，電子郵件訊息傳遞在

發訊端與收訊端對訊息需求有共識之下，此時我們就可以看作是一種福利極大的情況。因此電子郵件管制可以朝向從制度上創造出誘因；在質的部分，可使得發訊端能提供收訊端所偏好的訊息類型、或減少雜訊，在量的部分，則應致力於改變發送電子郵件邊際成本幾近於零之特質。

綜合以上，從市場機制上要來處理垃圾郵件這樣一種濫用傳輸工具之問題，第一步就是要導入價格機制於電子郵件服務提供。相較於行動通訊上垃圾簡訊問題嚴重性之差異，倘若能提高發送者增加發送一封訊息之邊際成本，或許可以對濫發者產生負面誘因。責任配置可以說就是制度誘因，而影響人類的行爲。在討論政策或法律問題時，市場的概念相對地有著一種未來性，意即採取哪一種政策或法律或判決，將會形成哪種誘因，在未來會引發那些行爲。據研究指出，目前垃圾郵件之組成，以行銷商品或服務爲目的而不請自來之電子郵件爲最大宗，也最無管制爭議（因爲管制者與中介端、收訊端大抵立場一致）。此正凸顯了垃圾郵件管制與一般網際網路內容管制之差異所在，與控制方式轉折的契機。故要在此間形成市場，則發訊端責任會是較符合效率與公平之選擇。從而，或配合認證技術發展，可對於有大量發送需求的行銷者，以收取相當費用來抑制其行爲，創造出合法電子郵件行銷之空間，如電子郵資[31]方案。其次，在中介端與收訊端部分，也可以嘗試發展出付費使用、客製化的電子郵件過濾服務市場，以改善前述所稱第三種意涵之網路結構。

---

[31] 今年一月曾公開受 Bill Gates 的倡議。類似的討論 See e.g., Ed Bride, Stamping out SPAM with E-Mail Postage, Security Innovator (Sept.29, 2003), available at http://securityinnovator.com/index.php?articleID=2038&sectionID=25 （最後瀏覽日期 2004 年 11 月 14 日）; Sonia Arrison, Canning Spam: An Economic Solution to Unwanted E-mail, Pacific Research Institute (Feb. 2004), available at http://www.pacificresearch.org/pub/sab/techno/2004/spam01-26-04.pdf. 不過，有認爲認爲由於此一方案對於所有類型之電子郵件皆有適用，，此一慣例建立，有擴大運用而相對地抑制電子郵件服務之使用以及限制訊息自由流通之疑慮。See e.g. Lessig＆Resnick, supra note 6, pp.428-429.

伍 結論

管制問題與管制環境之間是一種動態的交互影響關係。深入研究網際網路規範議題的 Lessig（2003: 1）曾表示：「在網路法領域，若相關管制措施欲達成預期效用，那麼就必須充分理解規則與技術間的互動關係。」本文則以爲還不僅如此。正如本文於一開始即表明了，當代網際網路的應用已經超越資訊交換層次，而更是現實世界經濟、政治、社會等活動之延伸。誠如法律經濟學的發展將效率觀點帶入規範分析之中，因而在當前網際網路領域規範此一領域管制議題之研究上，亦需充分理解科技、經濟與規範三方面間的互動關係。是以分析垃圾郵件管制問題，也不應忽略對於目前網際網路電子郵件傳輸結構的瞭解[32]。

以存取控制角度來分析垃圾郵件議題，意味著係將垃圾郵件問題，定性爲一種負面訊息傳播行爲來討論。除了凸顯管制垃圾郵件將不可避免觸及關於網際網路內容管制之爭議外，此一種分析角度，也能夠呈現管制垃圾郵件之規範困境以及實體法律與現今網路結構之扞格。由於在電子郵件訊息傳遞過程中，由沒有一方有完全的資訊、技術能力、及行爲誘因來承擔垃圾郵件管制之問題，故確實有管制之必要。然而，干預的力量，並不必然來自於政府，其干預點（管制點）之選擇，必須從網路結構可變動性出發，考慮各訊息端之技術能力、責任分配、及管制者成本之問題。

透過前文分析，大致可歸納出幾點垃圾郵件管制議題之問題：首先，當前電子郵件傳輸結構上，由於是一種單向與片面的訊息傳播型態，因此發訊端與收訊端在資訊自主權上，顯然處於控制力失衡之情

[32] Katyal（2003: 2288）肯定了 Lessig＆Resnick 的論點，並認爲對於網路內容的規範，過去美國實務與學界都過於重視立法管制而非其他如技術變遷之控制方案。Weinberg（2000）延續 Lessig＆Resnick 之管制思維，也反對對於一昧地朝向立法管制一途，提出以改變網路結構，或發展一能夠辨識訊息類型、收訊端特質與管轄的數位認證方案，以建立一個網際網路信任系統。

形。依訊息傳播模式而異其管制強度與控制點，特別是未能考慮管轄問題之傳統媒介管制架構，此時已難再適用。進一步分別探討垃圾郵件之存取控制後，發現：一、決定何爲垃圾郵件之適合點，係發訊端或收訊端；從理論上，收訊端控制較發訊端決定更加滿足資訊充分流動之要求，但卻將可能產生收訊端承擔高度成本、發訊端獲取超額利潤之不公平現象。而中介端則是在技術與風險分配能力上，優於前兩者。二、現今網際網路結構並不利於管制垃圾郵件規範之執行、使得各種責任歸則之執行成本高昂，而降低了管制效率。三、從管轄的因素來看，除了令發訊端無從判斷適用規則而正當發送訊息外，管制執行也將由於網路無國界之特質而致生障礙。因此能否透過國際產官合作而協調出較爲一致的垃圾郵件管制規則，將成爲未來垃圾郵件管制有效性的關鍵之一。

對於垃圾郵件之管制策略選擇，本文亦認同目前並無任何一種單一有效的執行方案。現階段之立法規範趨勢，其宣示意義大於實質效用；重點應在於國際間可以因此有具體的協調管制垃圾郵件策略之基礎。在現今網路結構下，在本地管轄中採取從嚴立法之選擇，本文以爲只是突然損傷法律尊嚴；反之，從國際共識之必要規則出發，管制強度由鬆漸密，反而減少因爲管轄因素所導致存取控制和執行障礙。考慮目前以過濾技術爲主的國際共通策略，或可同時將管制對象設定在發訊端與中介端，特別有必要給予後者制度性誘因，以創造出電子郵件服務之相關市場。本文認爲科技解決與市場機制方案，無論是在管制工具之多樣與管制點上，都深具發展性與彈性，但是也隱隱約約有著高度過濾後，有限制資訊流通之危險性存在。惟針對目前的一些治標不治本之立法與技術解決方案，本文以爲垃圾郵件發送技術與反制技術交相破解、競賽是無止盡之循環，除非調整網際網路結構—特別是改變電子郵件傳輸結構，方爲治本與提升管制效率之作法。

簡言之，本文在管制策略選擇上，偏好以弱化濫發行爲（數量問題）之誘因策略爲主，進一步才思考訊息類型（質）問題。後者可以加以發訊端之標示義務來處理，既免於過渡負擔、也滿足收訊端資訊之自主權。是以，能將濫發行爲之外部成本內化且強化收訊端控制之市場機制方案，應爲目前考量管制設計上歸責與懲處機制選定部分之主要研議方向。承前所述，在現有網路結構下不論管制點與責任配置如何，管制者都將面臨高昂的管制成本。故在不改變網路結構下，能夠設計出一協助追蹤垃圾郵件發訊端之市場，也是權宜之作法。而在未來網路結構改變下，則或可進一步考慮調整爲中介端與收訊端之控制。

垃圾郵件管制之政策窗已經開啓。本文以爲我國主管機關現階段除了在立法與管制策略決定上應注意此前所提出的規範設計問題。管制之目的在於消除市場失靈與資源使用的無效率，那麼未來所採取的管制措施之目標也應該要達成極小化因爲管制發送垃圾郵件這樣的經濟活動所帶來的社會無謂損失。對於目前實務界所發展出的技術解決方案，也不應一昧地爲求解決垃圾郵件問題，而忽略相關措施之負面效果。

附錄

比較國際垃圾郵件規範之主要內容

	美國	日本	澳洲	英國	加拿大	韓國
1.是否專以法規範 SPAM?	ˇ	ˇ	ˇ	ˇ	(立法中)	ˇ
2.法律或政令的名稱	CAN-SPAM Act	特定電子郵件法	Spam Act 2003	2003 隱私與電子通訊法令及指導綱領）	Spam Control Bill	促進資訊通訊網路利用及資料保護法
3.SPAM 的定義及範圍?	(Unsolicited) Commercial Adv. Electronic	Unsolicited Commercial Adv.	Unsolicited Commercial Electronic, and including mobile text	(Unsolicited) Adv. (marketing) Electronic, and including mobile text	Unsolicited Electronic	Commercial Adv. Electronic
4.對於 SPAM 有明確的排除對象?	ˇ	ˇ	X	ˇ	ˇ	X
5.主要規範對象	Sender&第三人	Sender	Sender	發信者&廣告主	Sender	Sender&廣告主
6.要求郵件主旨欄加註特別標示?	ˇ	ˇ	X	ˇ	X	ˇ
7. Opt-in 機制有無[33]	X	X	ˇ	ˇ排除法人 此外，例外僅採 opt-out 情形尚有三[34]	X	X
8.在郵件中要求 Opt-out 的選擇?	ˇ	ˇ	ˇ 排除政府部門、政黨、宗教組織、慈善及教育機構	ˇ	ˇ	ˇ
9.要求發信者之真實身份或位址?	ˇ 不要求揭露身份	ˇ	ˇ	ˇ	ˇ	ˇ
10.禁止錯誤信首資訊?	ˇ	ˇ	ˇ	ˇ	ˇ	ˇ

	美國	日本	澳洲	英國	加拿大	韓國
12.禁止為發垃圾郵件目的而蒐集或轉讓位址	ˇ	ˇ	ˇ	X	ˇ	ˇ
13.禁止為發垃圾郵件目的而使用郵件位址蒐集器或組合軟體	X	ˇ	ˇ	X	X	ˇ
14.建立 Do-not-spam list?	FTC 已依法向國會提出報告，但建議不建置	X	X（但有工業碼制度）	X（但有工業碼制度）[35]	ˇ	ˇ
15.明定 ISP 業者過濾機制的相關規範	X	ˇ	X	X	ˇ	X
16.明定給予 ISP 業者的免責條款	X	ˇ	X	X	ˇ	ˇ
17.刑事懲罰	ˇ	X	X	ˇ	ˇ	ˇ

資料來源：通訊傳播委員會籌備處，2004/06

參考文獻

Balkin, Jack M. (2004). “Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society,” *New York University Law Review*, 79: 1-58.

Jamieson, Paul (2004). “$TOPP^NG $P@M!!: The Private Sector Needs to Regulate Spam Because the Government Can’t,” *Legal Affair:* 23-24.

Katyal, Neal Kumar (2003), “Digital Architecture as Crime Control,” *Yale Law Journal*, 112: 2261-2289.

Kendrick, Joseph P. (2003), “"SUBJECT: ADV:"ANTI-SPAM Laws Force Emerging Internet Business Advertisers to Wear the Scarlet "S",” *Journal of Small and Emerging Business Law*,7: 563-576.

Lessig, Lawrence & Paul Resnick (1999). “Zoning Speech on the Internet: A Legal and Technical Model,” *Michigan Law Review*, 98: 395-431.

Lessig, Lawrence (1999). “The Law of the Horse: What Cyberlaw Might Teach,” *Harvard Law Review*, 113: 501-519.

Lessig, Lawrence (2003). “Law Regulating Code Regulating Law,” *Loyola University of Chicago Law Journal*, 35: 1-14.

McQuail, Denis and Sven Windahl (1993). *Communication models: for the study of mass communications*, New York: Longman.

Nyberg, Amy Oberdorfer (2004), “Is All Speech Local? Balancing Conflicting Free Speech Principles on the Internet,” ***Georgetown Law Journal***, 92: 663-688.

OECD（2004a）“OECD Workshop on Spam: Report of the Workshop,” DSTI/CP/ICCP (2004) 1, (http://www.oecd.org/dataoecd/55/32/31450810.pdf), 2004/03/11.

OECD（2004b）“2nd OECD Workshop on Spam: Report of the Workshop,” DSTI/CP/ICCP/SPAM (2004)7, (http://www.oecd.org/dataoecd/12/42/33800116.pdf), 2004/11/02.

Porter, Rebecca (2004). “Smothered by Spam, “ *Trial*, 40: 50-54.

Sorkin, David E. (2001). “Technical and Legal Approach to Unsolicited Electronic Mail,” *University of San Francisco Law Review*, 35: 325-384.

Trussell, Jacquelyn (2004). “Is the CAN-SPAM Act the Answer to the Growing Problem of Spam?” *Loyola Consumer Law Review*, 16: 175-188.

Weinberg, Jonathan (2000), “Hardware-Based ID, Rights Management, and Trusted Systems,” *Stanford Law Review*, 52: 1251-1281.

Zarsky, Tal Z. (2004). “Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society, *University of Miami Law Review*, 58: 991-1044.

太穎國際律師事務所（2003），《濫發電子郵件行爲之管理與法制規範研究 期末報告》，行政院經濟建設委員會委託研究，未出版。

王郁琦、陳炳全（2002），〈濫發網際網路廣告信相關法律問題之研究〉，《月旦法學雜誌》，第八十一期，頁 152-166。

唐慧文（2004），〈反垃圾郵件協定邁向整合〉，http://taiwan.cnet.com/news/software/0,2000064574,20084735,00.htm，2004/04/10。

陳思廷、郭佳玫、黃菁甯、林雅慧（2004），〈垃圾郵件的國際立法趨勢〉，《科技法律透析》，第十六卷第二期，頁 20-47。

陳奭璁（2004），〈垃圾郵件氾濫 SMTP 該壽終正寢？〉，http://taiwan.cnet.com/news/comms/0,2000062978,20082008,00.htm，2004/04/10。

劉靜怡（1998），〈網路社會規範模式初探〉，《臺大法學論叢》，第二十八卷第一期，頁 1-45。

劉靜怡譯（2002），Lawrence Lessig 原著，《網路自由與法律》，初版，台北：商周。

Study on the Analysis of Spam Regulation by Access Control Model

Lin, Meng-peng
Graduate Institute of Public Administration
National Cheng-chi University

Abstract

Despite legislative prohibition and anti-spam technical measures proposed by the internet service providers and specialists, the growth of spam continues incessantly. Spam is not merely anathema to nearly every publicly identifiable interest holder, but burdens the development and application of internet with the deadweight loss. Spam control, thus, also involves in the debate of the norm in cyberspace.

A model of access control is adopted to analyze spam regulation with the existing transmission protocol and spillover phenomenon. This article defines spam regulation as blocked information exchanges, and discusses which parties carry the responsibility for providing the information necessary for that blocking. As Lessig and Resnick point out that no one actor, at the outset, may possess all of that information. After analyzing these options, a better strategy is multi-approached, for the most part of market-oriented measures. This article concludes that by encouraging regulation designation to adopt a combination of the intermediary and sender's responsibility, the regulator can achieve greater certainty at minimal cost, while maximizing the flow of information in the present architecture.

Key words: access control, spam, the norm in cyberspace, spillover