濫發電子郵件行為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

太穎國際法律事務所　辦理

中　華　民　國　九　十　二　年　十　二　月　三　十　一　日

感謝序

太穎國際法律事務所辦理行政院經濟建設委員會財經法制協調服務中心委託，就濫發電子郵件行為之管理與法制規範議題進行專案研究。研究期間，感謝行政院經濟建設委員會財經法制協調服務中心給予我們多方的協助，張新永主任及何俊輝主任不吝指導與劉美琇組長、林倩如小姐積極協力連繫機關資源，都是本研究能順利開展的重要因素。

為明確獲悉我國網際網路服務業者在處理濫發電子郵件工作上面對的實際問題，本所在行政院經濟建設委員會財經法制協調服務中心支持下，邀請相關業者齊聚，就本研究主題深入探討。與會業者代表在會中與會後，分別以口頭與書面所做的資訊提供與意見反映，使本研究在我國實況部份的分析得以切題，並對本研究報告之結果有重要的影響，本所在此要特別向以下諸位業界先進致意：

王齊年經理　　台灣電訊股份有限公司
吳小琳協理　　數位聯合電信股份有限公司
吳興忠先生　　和信超媒體股份有限公司
李慶璜協理　　東森寬頻電信股份有限公司
周柏良經理　　亞太線上服務股份有限公司
侯彥安主任　　和信超媒體股份有限公司
秦承瑤總監　　雅虎國際資訊股份有限公司
郭智仁資深經理 新世紀資通股份有限公司
陳建榮資深經理 數位聯合電信股份有限公司
陳麗芳小姐　　中華電信股份有限公司
楊春華法律顧問 新世紀資通股份有限公司
廖國仲先生　　亞太線上服務股份有限公司
歐陽拾瓊組長　財團法人台灣網路資訊中心
鍾福貴處長　　中華電信股份有限公司

同時本所要感謝東方線上股份有限公司邱高生先生慨允提供我國網際網路使用行為的實證調查資料供本研究引用，使本研究報告之分析更加具體。

本研究報告於期中提出關於本研究主題之初步建議指向，以及國際研究進程成果，有幸獲得如下諸位審查委員的詳細審閱與回饋意見，使本研究報告能由更廣闊的層面周延掌握產官學各界對濫發電子郵件問題管理的重視與期望：

吳小琳協理　　數位聯合電信股份有限公司
范建得所長　　國立清華大學科技法律研究所
許慶齡顧問　　雅虎國際資訊股份有限公司
陳國龍副處長　　交通部電信總局公眾電信處
熊愛卿教授　　銘傳大學法律學系
戴豪君組長　　財團法人資訊工業策進會科技法律中心
羅正棠副研究員　行政院國家資訊通信發展推動小組科技顧問組

立法委員邱創進、邱太三及洪奇昌國會辦公室，在本研究報告截稿之前，舉辦以「如何立法管理垃圾電子郵件」為題的公聽會，本所律師忝列應邀發言者之列，恭聆與會專家對本研究主題發表的精闢言論，使本所有機會再一次檢視報告草稿全文及修正部分觀點。本所希望在此向當時在場主持公聽會的邱創進委員及到場指導的下列專家致上謝忱，也特別感謝邱創進委員辦公室尚道明主任與李清慧小姐協助整理與提供公聽會會議記錄作為本報告中極有價值的一份附件：
高凱聲博士　　交通部電信總局副局長
郭國燦副總工程師　中華電信股份有限公司數據分公司
郭聯彬先生　　蕃薯藤數位科技股份有限公司法務室
黃菁甯律師　　財團法人資訊工業策進會科技法律中心
劉美琇組長　　行政院經濟建設委員會財經法制協調中心
應冠群先生　　數位聯合電信股份有限公司

最讓本所全體投身本研究同仁感動且難忘懷的是，自二00三年七月起短短六個月的研究期間，國際間管制濫發電子郵件行為的立法運動，風起雲湧，快速建構起世界性的網際網路法制合作體系。本所同仁多次利用面訪、電話討論及電子郵件連繫，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；各位受訪者熱情而積極的回應，令我們十分慶幸本研究自開始就選取了正確的研究手段，而能有如此豐碩的收獲，本所因此要向下列先生及女士致上誠摯敬意：

Greg Abbott
Attorney General for the State of Texas
USA

Lindsay Barton
Manager of Online Privacy, National Office for the Information Economy
Commonwealth of Australia

Hyu-Bong Chung, Ph. D.
Vice President of the Korea Information Security Agency (KISA)
Republic of Korea

Stephen Collins, Ph.D.
Director of International Public Policy, Yahoo! Inc.
USA

Mike Honda
Representative for the Fifteenth District of California
United States House of Representatives
USA

Phil Kline
Attorney General for the State of Kansas
USA

Lawrence Lessig
Professor of Law at the Stanford University School of Law
USA

James Lick
Chair, Asia Pacific Coalition Against Unsolicited Commercial Email
Taiwan

Erkki Liikanen
EU Commissioner for Enterprise and the Information Society
Belgium

Steve Linford
The Spamhaus Project
United Kingdom

Bill Lockyer
Attorney General for the State of California
USA

Zoe Lofgren
Representative for the Sixteenth District of California
United States House of Representatives
USA

Kate Lundy
Senator for the Australian Capital Territory and
Shadow Minister for Information Technology
Commonwealth of Australia

Andrew Miller
Member of Parliament and
Treasurer of the All Party Parliamentary Internet Group
United Kingdom

Ron Paul
Representative for the Fourteenth District of Texas
United States House of Representatives
USA

Brian Sandoval
Attorney General for the State of Nevada
USA

Steven M. Sakamoto-Wengel
Assistant Attorney General/Deputy Chief, Consumer Protection Division
Attorney General for the State of Maryland,
USA

Paula Selis
Senior Counsel, Attorney General for the State of Washington
USA

David E Sorkin
Associate Professor of Law, The John Marshall Law School
and Creator of the website: www.spamlaws.com
USA

William H. Sorrell
Attorney General for the State of Vermont
USA

Brian White
Member of Parliament and
Treasurer of the All Party Parliamentary Internet Group
United Kingdom

Daryl Williams, AM QC MP
Minister for Communications, Information Technology and the Arts
Commonwealth of Australia

Ron Wyden
Senator for the State of Oregon
USA

本研究已經開啟了在此一重要的網際網路新興議題上可觀的國際合作實踐。本所懇切期待本報告內容能裨益於我國立法、行政、司法各部門相應措施之落實及民間企業自律，網際網路使用者權益保護同時達致國際一流水準。

太穎國際法律事務所
謝穎青

2003年12月18日

研究摘要

一、研究背景及方法

網際網路服務普及以來，利用電子郵件為行銷通路的現象亦隨之氾濫，竟而演變成所謂「Spam」這個新名詞產生。「Spam」（有譯為「垃圾郵件」者）概括描述種種濫發電子郵件的行為，實已造成電子郵件之使用者使用上之不便及網際網路服務提供者（ISP）經濟上之損失。

本研究藉由「文獻探討」及「意見彙整」等社會科學研究法，採取文獻蒐集、業者及各國主管機關之深度訪談、舉辦座談會等方式，以探討濫發電子郵件之意義為出發點，分別就法制面、政策面及實際執行面等三大面向進行分析，並針對如何有效規範與解決電子郵件濫發行為提出相關報告與建議，作為我國爾後相關政策制定與處理機制建立之參考。

二、研究重要發現

本研究在研究過程中獲致許多重要發現，首先關於濫發電子郵件之定義、態樣及問題方面，本研究藉由外國法例之研究及電子郵件之性質，勾勒出濫發電子郵件之定義，大致可分為非請自來的大量電子郵件（unsolicited bulk e-mail，簡稱為 UBE），以及非請自來的商業電子郵件（unsolicited commercial e-mail，簡稱為 UCE）；同時本研究亦蒐集歐盟、日本、韓國及澳洲相關法令關於濫發電子郵件之定義以供參酌。

在濫發電子郵件引發之問題中，本研究詳述了其造成財產上之損失及其他影響，包括：造成企業與網路社群生產力成本之大幅增加、具爭議性之內容、浪費網路資源、危害電子商務交易及資通安全、影響網路使用者之信心等。在目前世界各先進國家管制濫發電子郵件之管理機制方面，本研究分別從科技、市場及法律等解決方式逐一探討其良窳。本研究發現雖然科技及市場之解決方式有助於管制濫發電子郵件，惟法制面之完備，仍有其必要性及正當性。

本研究分別整理歸納美國、歐盟及亞太地區國家如日本、韓國、澳洲等國對於電子郵件濫發行為相關法令、政策暨管制措

施、法律草案、法規界定及相關訴訟案例，尤其是美國之聯邦及各州法律、法院實務見解及損害賠償之理論，及最近美國之立法動態，在防制濫發電子郵件之研究方面，已累積一定之案例及理論學說，足供我國借鏡。

三、結論與建議

本研究認為：濫發電子郵件帶來的問題，並不是只有一個；完全禁絕濫發電子郵件現象，事實上並不可能。但是，在一定期間內有效減少濫發電子郵件之數量，以及遏止濫發電子郵件散佈之不法內容與電腦病毒，確實可能透過執行適當法律，鼓勵網路服務業者採取積極預防作為，以及教育企業經營者與消費者正確看待網路行銷的觀念來實現。貫串這一種多管齊下模式而奏功的關鍵，則是多邊的政府間國際合作。

本報告依此建議：

一、 修訂現行保護隱私及交易安全的法令，將保護擴及於制止濫發電子郵件可能帶來的實害及經濟損失，並考慮賦予 ISP 業者法律上權利，阻止濫發電子郵件散佈。

二、 制定特別法一舉涵括處理濫發電子郵件產生的社會法益與個人法益侵害問題，亦屬可行選項，而規定：

（一）認定濫發電子郵件標準建立；
（二）如何禁止發送濫發電子郵件；
（三）賦予網路使用者拒收選擇權，以採事前同意機制(opt-in)為宜；
（四）廣告主及發信人應於電子郵件納入"商業"或"廣告"等標示，以利收件者選擇過濾；
（五）ISP業者主動或被動之義務過濾；
（六）虛偽發信來源或規避行為之防制；
（七）強制廣告主提供真實資訊，例如正確發信來源與聯絡方式，俾收件者回覆、爭訟或提出要求；
（八）損害賠償額度、舉證責任分配及研析禁止騷擾性訴訟可能性；
（九）發送濫發電子郵件行為犯罪化之優劣研析；
（十）管轄權與審判地決定。

三、行動電話網路上已出現或可能濫發之廣告簡訊，目前市場收費機制以及電信業者配合主管機關督導所實施的防制措施，已見成效，本報告建議可以保留觀察。

四、 成立專責主管機關積極參與國際合作。從濫發電子郵件之本質為行銷行為觀之，我國主管濫發電子郵件之專責主管機關應為公平交易委員會（例如在美國為聯邦貿易委員會負責）。但從電子郵件傳輸之管理觀察，則應由交通部電信總局或將來成立之資訊通訊傳播委員會（例如在澳洲為通訊署）主管。不論如何，專責隱私保護主管機關(依將來修訂完成之個人資料保護法，將是法務部及各目的事業主管機關)在本主題上，與上述經決定後之主管機關並肩工作，一起投入與鄰國及世界主要市場間之多邊規範或合作方案協調，勢必不可或缺。當務之急尤應立即回應亞洲太平洋地區已經對我國表達合作打擊濫發電子郵件誠意之國家，建立共通行動準則。

關鍵字：濫發電子郵件、垃圾郵件、電子商務、網際網路、隱私、電子通訊

EXECUTIVE SUMMARY

Problems Associated With Spam

Internet service provider America Online has reported that it filters out more than 2 billion spam e-mails per day. Brightmail, a company that provides spam-filtering technology to MSN, Hotmail and other companies, announced that its filters are used to block more than 60 billion spam e-mails per month. This deluge of spam is more than just an annoyance. According to some research groups, spam will cost businesses more than US $20 billion worldwide in 2003.

Spam causes various problems including annoyance, fraud, loss or delay of legitimate messages, consumption of bandwidth and storage space, strain on servers, lost productivity, costs of additional equipment and personnel, spoofing, consumer complaints and possible hostile working environment. All of the problems can be placed into one of two categories: those caused by spam volume and those caused by content. Unwanted pornography and fraudulent spam are problems of content. However, most of the problems – and most of the monetary damages that result from spam – are caused by volume. The volume of unwanted messages is what causes lost productivity for businesses, consumption of bandwidth and storage space and strain on servers; volume is what forces ISPs and companies to obtain additional equipment and personnel to block the flood of unwanted messages; and volume is the primary cause of frustration and complaints by consumers, businesses and ISPs. Most authorities therefore agree that the primary goal of spam legislation should be to reduce the volume of spam.

International Legislative Approaches

Most spam legislation falls into one of two categories: opt-in or opt-out. Opt-in legislation prohibits the sending of unsolicited commercial e-mails, or UCE, without the recipient's prior consent. Opt-out legislation allows one to send unlimited UCE, but each message must contain a feature allowing the recipient to respond and request that the sender stopping sending UCE to that particular address. There seems to be a consensus among experts that opt-in

legislation will be more successful at reducing spam volume than opt-out. Those who send fraudulent spam will likely ignore any spam laws, they say, but opt-out legislation legitimizes UCE and will lead to a dramatic increase of UCE from “legitimate” businesses. Opt-in legislation is being adopted in Europe and Australia; opt-out is the approach of the United States.

In Europe, EU Directive 2002/58/EC, dated July 12, 2002, requires all EU Member States to enact opt-in legislation consistent with the Directive by October 31, 2003. According to the Directive, no person may send UCE to an individual without prior consent. Actually, the Directive is referred to as a “soft opt-in” law because it contains one major exception. UCE is permitted where the sender received the recipient’s e-mail address during a sale or negotiations for a sale of goods or services that are the same or similar to those which are being offered in the UCE. In addition, the EU Directive prohibits any person from disguising or concealing his identity when sending UCE and requires all UCEs to include a valid return address that enables the recipient to opt-out of receiving UCE in the future. Six EU Member States – Austria, Denmark, Ireland, Italy, Spain, and the United Kingdom – have enacted opt-in spam laws implementing the Directive as required. Seven States have not yet enacted appropriate legislation and the EU has asked them to explain within two months how they intend to comply with the law or face possible court action.

While it is not a member of the EU, Australia has also promulgated an opt-in version of spam legislation in its Australian Spam Bill 2003 which was passed in December 2003. Like the Directive, the Spam Bill prohibits sending UCE without prior consent. Unlike the Directive, the Spam Bill does not make an exception where the sender received the recipient’s address during a prior or ongoing sale or negotiations. Instead, the law makes an exception where the sender has either express consent or consent that can be inferred from conduct or business relationships. The Australian standard is similar but slightly more vague (and therefore a possible loophole for spammers). The Australian Spam Bill also includes exceptions for e-mails sent from government, political, religious, charitable and educational entities.

On the other side of the spectrum, the U.S. is on the verge of enacting opt-out legislation known as the CAN-SPAM Act. Under

CAN-SPAM, one may send unlimited UCE, so long as each message contains a feature allowing the recipient to opt-out of receiving further UCE. In addition, CAN-SPAM prohibits false or misleading header information or subject lines, requires UCE to be identified as advertising (although it does not require any particular form of identification) and prohibits any display of sexual content on the first page that is visible when opening UCE (the first page may contain a link to such content).

One of the controversial provisions of CAN-SPAM is the do-not-spam registry, where Internet users could submit their names if they wish to opt-out of receiving all UCE. CAN-SPAM does not actually require that such a registry be created, however, but just that the FTC investigate that possibility. The Act also contains another interesting provision, a potential system of rewards to be paid to those who give information leading to the prosecution of spammers. Another controversy of CAN-SPAM is that it does not give a private right of action for enforcement to individuals who are harmed by spam; instead, it may be enforced only by ISPs and certain state and federal entities. Many feel a private right of action is necessary to effectively address the spam problem.

Recommendations for Taiwan

At Article 4 of the Computer-Processed Personal Data Protection Law, Taiwan has taken an opt-out approach: a person may not waive in advance the right for others to obtain, review and use that person's personal data. It would be a serious mistake for the government of Taiwan to also adopt an opt-out approach with regard to spam legislation. Most of the problems caused by spam are due not to its content but its volume. The tremendous volume of UCE causes not just annoyance, but also substantial monetary damages and the volume of UCE seems to be growing incrementally. Because spam experts almost universally agree that opt-in legislation will be more effective at reducing spam volume than opt-out, that first decision is clear: Taiwan should enact opt-in spam legislation.

After that, there are a number of standard provisions in international spam laws that would benefit Taiwan: the use of false or

misleading information in the header of subject lines of UCE should be prohibited; even when a person consents to receive UCE, that UCE should be required to include an opt-out feature; UCE should also be required to include a clear label in the subject line, identifying it as UCE (preferably in a standard required format); use of automated means to harvest e-mail addresses from websites or to randomly create addresses for recipients of UCE should be prohibited; the law should provide statutory damages in amounts great enough that they are not just another small “cost of doing business”; and the law should authorize enforcement not just by the government, but also by ISPs and by any person or entity that is injured by a violation of the law.

Only by enacting strong anti-spam legislation such as the above can Taiwan expect to see any reduction in the significant damages and annoyance caused by spam. Without such legislation, the problems will only grow worse.

目錄

圖表次

附件

附件一　各 ISP 業者參加【ISP 業者對濫發電子郵件之建議與期許座談會】之書面回應整理表

附件二　交通部電信總局「撥接連線網際網路接取服務定型化契約書範本」

附件三　訪問雅虎國際公共政策總監 Dr. Stephen Collins 對濫發電子郵件問題之訪談紀錄 (2003 年 10 月 1 日)

附件四　訪問韓國國家資訊安全局個人資料爭議委員會秘書長 Hyu-Bong Chung, Ph.D.有關管理濫發電子郵件問題之談話紀錄
(2003 年 10 月 1 日)

附件五　訪問英國國會議員 Brian White, MP（Member of Parliament in the United Kingdom and Treasurer of the All Party Parliamentary Internet Group）有關管理濫發電子郵件問題之談話紀錄
(2003 年 11 月 6 日)

附件六　美國聯邦有關管理濫發電子郵件相關法案
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003(or the “CAN-SPAM Act of 2003”).

附件七　美國加州有關管理濫發電子郵件相關法案
California Business and Professions Code Division 7, Part 3, Chapter 1 , Article 1.8. Restrictions On Unsolicited Commercial E-mail Advertisers

附件八　美國緬因州有關管理濫發電子郵件相關法案
Maine Revised Statutes, Section 1497.

附件九　美國密西根州有關管理濫發電子郵件相關法案
Michigan Public Act 42, House Bill 4519　(Approved July 11, 2003; effective September 1, 2003)

附件十　美國內華達州有關管理濫發電子郵件相關法案
Nevada Revised Statutes sec. 41.705, et seq., and sec. 205.492, et seq.

附件十一　美國維吉尼亞州有關管理濫發電子郵件相關法案
Virginia Code, Title 18.2, Crimes and Offenses, sections 18.2-152.2, 152.3:1, 152.4, 152.12 & 152.16 (2003)

附件十二　美國華盛頓州有關管理濫發電子郵件相關法案
Revised Code of Washington, Title 19, Business Regulations, sec. 19.190.010, et seq.

附件十三　美國西維吉尼亞州有關管理濫發電子郵件相關法案
West Virginia Code,
Chapter 46A, Consumer Credit and Protection Act, Article 6G, Electronic Mail Protection Act, sec. 46A-6G-1, et. seq., Added by Acts 1999, chapter 119, House Bill 2627

附件十四　日本特定電子郵件法

附件十五　日本特定商業交易法修正法案

附件十六　“Anti-Spam Regulations in Korea”
by Hyu-Bong Chung,Ph.D (2003 年 3 月 28 日)

附件十七　“Online Stamp System — Long and Serious Way to Fight Against Bulk Email”
by Yonnie Kim (Daum Communications, South Korea/AP, Net Abuse Workshop (2003 年 2 月 23 日)

附件十八　澳洲有關管理濫發電子郵件相關法案
A Bill for an Act about Spam, and for Related Purposes

附件十九　歐盟 97/66/EC 電信部門下之個人資料處理及隱私權保護指令
Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.

第一章　研究背景及問題提出

壹、　研究動機及目的

網際網路服務普及以來，利用電子郵件為行銷工具的現象亦隨之泛濫，竟而演變成有所謂「Spam」這個新名詞產生。「Spam」，本研究中譯為濫發電子郵件，有譯為「垃圾郵件」者，概括描述種種濫發電子郵件的行為，間及包括大量傳送色情詐財等不當內容郵件之情形，實已造成電子郵件之使用者使用網路服務之嚴重不便及網際網路服務提供者（ISP）實質上之損失。

所謂「濫發電子郵件」，本研究定義其為未經收信人請求「不請自來」之電子訊息，這些電子訊息外觀上涵括了一般人熟知的電子郵件、手機簡訊以及圖案鈴聲檔案下載等等。但是，以電子郵件為例，從發送的電子訊息內容上來看，又可區分為兩種態樣：一為UCE（unsolicited commercial email），係未經收信人許可而逕行遞送的商業性質電子郵件；另一種為 UBE（unsolicited bulk email），指未經收信人許可而大量遞送的電子郵件，在此種態樣強調的是數量，而非郵件的內容(即不僅僅限於商業廣告，其他諸如宗教性、政治性、問卷調查、種族議題、甚至色情等等皆包括在內) 。由於發信人短時間內寄發大量電子郵件，常常造成網路及電腦系統負擔過重。事實上相同的困擾現象也發生在無線及行動電話網路應用發達的國家與地區，包括美國、歐洲、及亞太地區使用行動電話手機或呼叫器等無線接取裝置的民眾，時常受到不請自來簡訊及圖案傳送騷擾，甚至受有財產上損害的比例快速升高，也是世所矚目廣義的濫發電子訊息現象。

根據資訊科技專業市場調查機構 Gartner 公司的分析指出，到 2004 年第二季為止，濫發電子郵件將佔去全球 60％的電子郵件收發量，大幅高過目前統計的五成，如此氾濫，不僅將使目前已造成網路塞車的狀況更形嚴重、業者與網路使用者防堵與篩檢這些不受歡迎的電子郵件成本提高、郵件管理更加困難，同時也將迫使網路商業正常運用電子郵件行銷變得窒礙難行。

上述報告明白指陳，越來越多的網際網路服務提供者（Internet Service Provider, 以下簡稱ISP）[1]、入口網站以及網路安全軟體業

[1] 依交通部電信總局制定之「撥接連線網際網路接取服務定型化契約書範本」第一條規定，網際網路服務提供者係指提供承租人撥接連線網際網路接取服務及其他相關服務之人。

者，採取針對所有疑似濫發電子郵件進行全面防堵，嚴格篩選的措施，逐漸使得正當廠商在發送行銷信件到合法取得的電子郵件地址時，同樣吃上閉門羹，此問題若無法獲得合理解決，到了 2005 年，將有 80％的行銷用途電子郵件還未送達就被封殺。再根據美國聯邦貿易委員會(Federal Trade Commission)於 2003 年 5 月進行的調查發現，有多達三分之二的行銷、廣告類電子郵件，不是誇大不實，就是有詐財之嫌，另一方面該會調查也發現，ISP 業者每天代收的電子郵件幾乎有三成屬於濫發電子郵件，預估 2003 年全年美國將耗費一百億美元於類似濫發電子郵件的防堵工作。由此可見，該如何管理濫發電子郵件已成為全球各電子商務先進發展國家當務之急。

針對這項嚴重問題，行政院經濟建設委員會積極預謀解決之道，先於 2003 年 4 月 18 日舉辦「網際網路經營與法制座談會」，蒐羅各界意見，並冀望透過委外研究案之辦理，就因應方式及法規修訂方向獲得具體建議。由於濫發電子郵件之行為，實有礙網際網路之秩序及電子商務之發展，世界各國已著手研究規範濫發電子郵件之行為，我國為發展電子商務，全力推動「數位台灣計劃」，更有必要針對濫發電子郵件行為建立適宜規範。太穎國際法律事務所爰接受行政院經濟建設委員會委託辦理本研究，分析歸納各國有關濫發電子郵件行為之管理與法制規範，作為我國制定相關法制之參考。

貳、研究架構

基於前揭問題與目標，本研究自濫發電子郵件之定義為探討起始，分別就法制面、政策面及實際執行面等三大面向進行分析，並針對如何有效規範與解決電子郵件濫發行為提出報告與建議，作為我國相關政策制定與處理機制建立之參考：

一、法制面

本研究彙整美國、歐盟及亞太地區的日本、韓國及澳洲等網際網路建設與電子商務應用已經進入高度發展之國家，其對於電子郵件濫發行為有無相關政策暨管制措施、法律草案、法規界定及相關訴訟進行研究，進而歸納各先進國家之相關具體做法以為本研究結論與建議提具之參酌。

二、政策面

本研究就我國當前濫發電子郵件之管制機制、相關可能適用之法規政策及目前立法院審議中之立法草案進行綜整探討，並輔以外國實務作為進行分析。

三、實際執行面

本研究結合我國實務面上 ISP 業者管理濫發電子郵件之經驗、個人資料之保護與相關適用法規執行狀況等，進行綜整分析，提具一套消費者利益、政府機關施政目標及商業需要可以兼容並蓄之法制規範與執行方案建議。

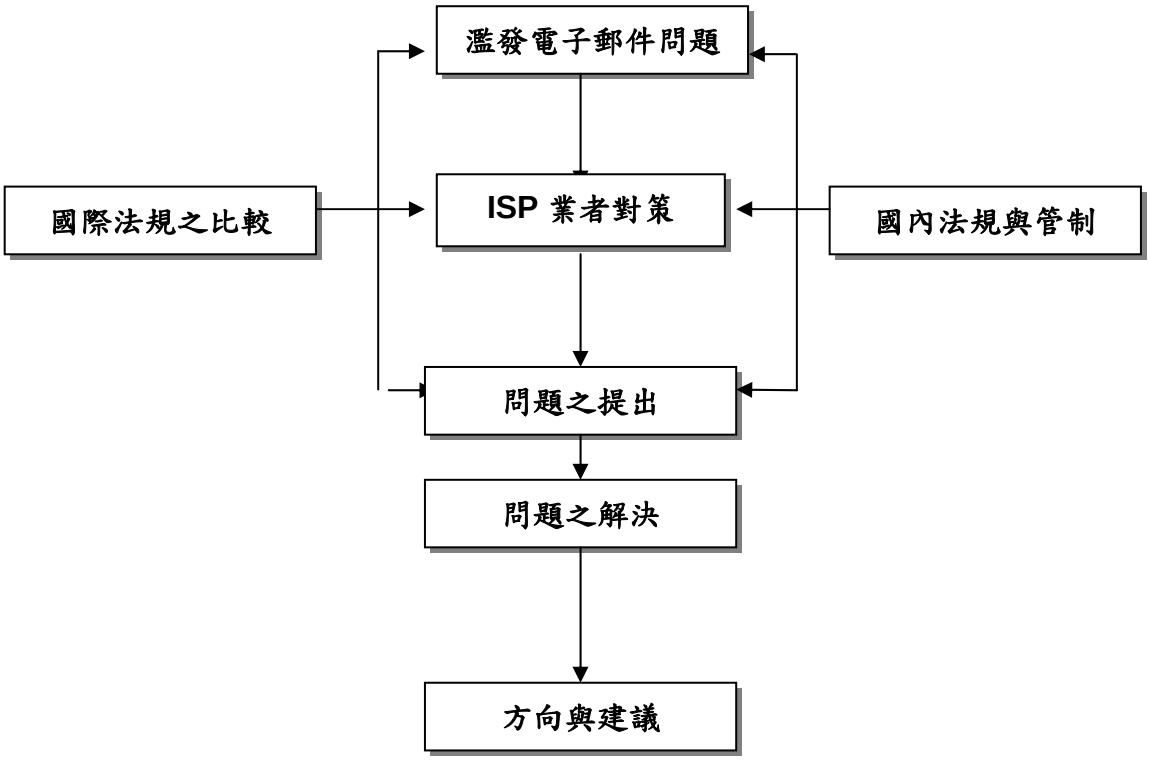


圖 1.1 濫發電子郵件研究架構圖

依前揭研究架構，本研究內容依序為：

一、濫發電子郵件之定義與問題

就當前全球主要先進國家及我國之網路使用狀態，以及因電子郵件濫發行為所產生之問題進行資料彙集，作為本研究主要之背景陳述。

二、各國對於濫發電子郵件行為之管制政策與措施研究

本研究特別針對美國、歐盟及亞太地區如日本、韓國、新加坡與澳洲等國，對於濫發電子郵件行為之管制與法規制定方向進行資料蒐羅與彙集，重點分別置諸於各觀察對象之法規體制、管制政策發展沿革、具體之執行方式及執行之成果等，並針對各觀察對象之法規政策進行比較分析。

三、我國對於濫發電子郵件行為之管制現況探析

本研究先就我國當前面臨濫發電子郵件行為現況予以整理介紹，再就我國相關之政策法規執行現況進行探討，最後輔以學者論著及 ISP 業者之意見與現況陳述。

相對於在技術層面針對濫發電子郵件所帶來之困擾發展各式各樣的解決方案，本研究更側重分析歸納各國法律規範，尋求有效對策，以期減少濫發電子郵件所帶來之問題。本研究將介紹美國、亞洲、歐洲等國為解決濫發電子郵件所為之立法及規範、相關之法律訴訟、其他可適用之法律、及正在審議中相關立法草案外，並將逐一檢討我國現有之法令，進一步申論是否我國須針對濫發電子郵件之問題作一個創新的立法規範，或者，依照現有法令，已足夠因應濫發電子郵件所造成之問題。

參、研究方法及進行步驟

本研究所採行之主要研究架構為由鉅觀至微觀、由外而內之分析方式，分別依據濫發電子郵件之問題，各國管制濫發電子郵件之法制，以及現今國內法規之適用及草案評析進行探討；而為求研究能更具宏觀、且臻完善可行，本研究亦規劃自法制層次以外其他技術層面及市場層面之分析思考，進行資料之彙集研析，

最後就我國當前法制面之罅漏與瓶頸綜整進行分析，藉以研析與提具我國未來法規制定之方向。

依據前揭研究之架構規劃，本研究規劃採行之研究方法主要有「文獻探討」及「意見彙整」，茲分項陳述如下：

一、文獻探討

資料彙集與研析於本研究中佔了極重要之部分，本研究針對電子郵件濫發行為之管理所進行之資料蒐集與整理，包含下列兩個面向與工作：

（一）國際研究：

本研究蒐集美國、歐盟及亞太地區如日本、韓國、新加坡、澳洲等國家之電子郵件濫發行為管理作為與法令政策進行蒐集分析，以為後續我國電子郵件濫發行為之管理法規與政策制定之借鏡。但是，囿於研究計劃時間之限制，本研究收集資料期限至 2003 年 12 月 25 日止，後續新增各國相關法案，將在日後另行增列為附件，以供參酌。

（二）國內研究：

蒐集國內現今電子郵件濫發行為之情形、針對該行為可堪適用之法令規範等資料，據以提具我國濫發電子郵件行為相關規範與政策制定建議。

二、意見彙整

本研究分別就當前市場現況、消費者爭議以及法規訂定等相關面向，藉由與外國相關主管機關官員之訪問對談，以及於國內針對 ISP 業者進行深度訪談與意見彙整，綜整該結果與資料，歸納出相關具體建議，作為本報告結論與管理機制研提及政策修正方向之建議。

肆、研究問題

關於大量濫發電子郵件之相關問題，本研究歸納後，分述如下：

一、濫發電子郵件之定義為何？濫發電子郵件所造成之影響及目前之對策為何？

二、各國對於管制濫發電子郵件之政策或法制為何？有無獲致具體成效？

三、我國目前對於管制濫發電子郵件之政策或法制為何？有無闕漏不足或窒礙難行之處？

四、我國目前有無參照外國立法例修正現行法令或另外訂定特別法以解決濫發電子郵件現象之必要？

五、我國應如何管制濫發電子郵件之行為？具體之執行事項為何？如何落實？

伍、預期結論

本研究預期分析完成之結論如下：

一、針對目前濫發電子郵件現象提供一個明確可供判斷之定義，並就其所造成之損害程度及影響層面提供評估；

二、就各國管制濫發電子郵件之法制提供一詳實之描繪及比較；

三、就目前我國現行法制及法律草案是否得以有效規範濫發電子郵件行為，提供法律見解；

四、就法制面以外之其他解決方式逐一檢視分析，並綜整提供具體可行性之建議，作為未來政府主管機關、ISP 業者及消費者保護團體之參考。

第二章　濫發電子郵件行為的管制機制

壹、關於濫發電子郵件之定義

網際網路應用蓬勃發展，商業經營者透過大量寄發電子郵件進行商品或服務有關之訊息傳遞或散佈廣告之行為日漸普遍，其中，許多資訊並非消費者所願意接收者，且實際上已經造成網路使用者以及 ISP 業者在處理時間上之浪費及金錢上損失，此類未經請求任意發送之電子郵件（unsolicited electronic mail），一般稱為 Spam mail，或俗稱為「垃圾郵件」。

一、濫發電子郵件之描述性定義

為了能夠清楚描述上述所謂未經請求任意發送之電子郵件現象，本研究將有關此現象之眾多定義大約歸納成下列兩種：不請自來的大量電子郵件（unsolicited bulk e-mail，簡稱為 UBE），以及不請自來的商業電子郵件（unsolicited commercial e-mail，簡稱為 UCE）：

-「不請自來的商業性電子郵件」（UCE，unsolicited commercial e-mail），係未經收件者事前許可或同意，就逕自對其大量遞送內容為商業性質的電子郵件，類似於一般常見的投寄至家庭或企業信箱的某些直銷刊物，同樣都是未經收件者的同意而寄發郵件，不同的是，在前者較難查出此郵件是否為未經請求而寄送的郵件。

-「不請自來的大量電子郵件」（UBE，unsolicited bulk e-mail），同樣是未經收件者事前許可而對之大量寄送的電子郵件，強調的是數量，而非郵件的內容(不僅僅限於商業廣告，其他諸如宗教性、政治性、問卷形式、種族議題、色情等等皆包括在內)，由於發信人往往在短時間內寄發大量電子郵件，經常造成 ISP 業者網路系統設備負擔過重甚而出現當機情形。

網際網路的匿名效應，造成了上述不請自來郵件在網路使用人無節制地使用轉寄功能而在網際網路流行，在網路商業抬頭的同時，利用電子郵件免費以及可以一對多大量傳送特性，所發展出的電子郵件行銷模式，更一舉將「不請自來的大量電子郵件」，在構成比例上大幅轉為大量「不請自來的商業性電子郵件」。結合了發信人匿名，以及以不法或不正當手段在網際網路內外蒐集網路使用者電子郵件地址兩個特徵，「不請自來的商業性電子郵件」(UCE)更加被污名化，突出而取代「不請自來的大量電子郵件」(UBE)，成為眾人聲討厭惡的對象。進一步也成為各國政府管制的客體。本研究借用美國法實務上對 UCE 及 UBE 的分析在此詳細描述二者之間的區別。

所謂的「不請自來」（unsolicited），依照與美國最多州法規定類似的加州州法規定，是指該不請自來的電子郵件被寄送到收件者時，除了未經收件者先前之明示同意外，收件者與發信人也不具備任何既有的或將來的商業或私人聯繫關係，而且發信人發送郵件之目的也不是在履行（collecting）現存的義務[2]。

上述收件者明示之同意，不能只是收件者消極之行為，例如收件者在Usenet貼文章，或單純拜訪發信人的網站並不構成同意之行為[3]。因此，並非所有未先同意收件的電子郵件均屬之，例如久未聯絡的老友或親戚寄來的電子郵件，即不在此範圍內。而賓州法律則是對不請自來的定義作了一個更加嚴格的規定，若發信人不是基於一個已經成立的商業關係上而寄送郵件，即有可能已經構成「不請自來」[4]。至於德州法律，則將不請自來定義成：除了對會員（members）、員工（employees）或立約者所發送的電子郵件外，所有以電子郵件傳遞的訊息皆可構成不請自來的信件[5]。

大量性（bulk）與商業性（commercial）之區別實益，是由於在美國商業性言論與一般性言論所受到憲法言論自由保護之強度不同，因此，規範濫發電子郵件的法律有無可能違背美國憲法第一條修正條文之機率也不同。尤其是在內容涉及到政治、宗教等議題的電子郵件，若立法限制其散發此類言論的自由時，該法

[2] See *California Assembly Bill 1629*，Sec2.；*Washington House Bill 1037*, Sec. 1(8)
[3] LINX(London Internet Exchange) Best Current Practice for Combating Unsolicited Bulk Email，seeHttp://www.linx.org/noncore/bcp/ube-bcp.html (visited on 2003/09/22)
[4] See *Pennsylvania Consolidated Statutes*, sec. 2250.2.
[5] See *Texas Statutes, sec*. 46.001(9).

違憲的可能性就會非常的大。一般來說，須發送到何種數量的電子郵件才能構成大量的地步，並沒有一個明確的標準可言，多數視各家ISP業者各自之規定而定，有些ISP業者對大量郵件的數量定有門檻，若二十四小時內寄給二十五位或以上的收件者即為大量[6]。

至於所謂商業性（Commercial），則是指包含遞送營利機構的銷售資訊、商品或服務的要約洽定、資金移轉要約或非營利機構的商業性活動等訊息的電子郵件。例如來自於各公司行號（包括網路公司）或個人之有關推銷產品、服務等等資訊的電子郵件，均屬之。UCE與UBE最大不同之處，在於UCE將其範圍限縮在內容須包含有商業訊息，而未含有商業訊息的郵件，則包括例如慈善團體的勸募函、宗教團體拯救靈魂之訊息，及非營利機構之非商業性活動訊息等郵件。由於UCE的定義未若UBE來得廣泛及漫無邊際，因此在美國實務上應用，UCE也較UBE的接受程度來得廣[7]。

二、關於濫發電子郵件之法律上定義

世界各國已有立法規範上述類如不請自來的大量電子郵件者，都是針對UCE，而非UBE。但是，各國法律對UCE賦予定義，因為政治、經濟及文化、歷史等不同國情考量，也有寬嚴程度不同的區別。以下謹列幾個代表性國家有關法律對於受規範UCE所做定義，供為參考：

(一) 歐盟

歐盟於 2002 年 7 月 12 日通過「歐盟隱私與電子通訊指令」(Directive on Privacy and Electronic Communications 2002/58/EC)，其中關於「電子郵件」(electronic mail, 第二條）之定義係指「透過公眾通訊網路寄送之任何文字、聲音、影像等訊息，且該訊息可以被儲存於網路或收件者之終端設備直到被開啟。」至於所謂「未經邀約商業訊息」(Unsolicited Communications,第十三條)，指「未經事前同意，而以語音電話、傳真或電子郵件等訊息為直接行銷。」

[6] The Mail Abuse FAQ, see http://www.members.aol.com/emailfaq/emailfaq.html (visited on 2003/09/22)

[7] 計有California、Kansas、Michigan、Minnesota、Washington等州對spam採取UCE之定義。

(二) 美國

CAN-SPAM Act of 2003 規定所謂「商業電子郵件訊息」（Commercial electronic mail message）係指：

- 任何主要以商業廣告或促銷方式行銷商業產品或服務之電子郵件訊息；
- 包括內含以行銷為目的之網頁；
- 不含交易或維持現有關係之訊息(transactional or relationship message)；
- 不含僅有營利事業網址連結之訊息。

(三) 日本

日本於 2002 年 4 月 11 日通過，同年 7 月 1 日生效之「特定電子郵件法」規定，特定電子郵件之定義係指限於商業電子廣告郵件，且發信人與收件者間並無契約、商業往來或其他法律關係。

(四) 澳洲

澳洲 Spam Bill 2003 中規定，所謂「電子訊息」(electronic messages)係指「使用網際網路傳輸服務或 1997 年電信法所列之傳輸服務，將訊息傳至電子郵件信箱或電話號碼等相類帳號者。」至於「商業電子訊息」係指「以下列銷售客體為要約、促銷廣告或其供應商之廣告或促銷為內容之電子訊息：

-商品或服務；
-土地；
-商業投資；或
-協助他人以詐欺或不正當手段取得財產或利益之訊息者。」[8]我國目前並無相關法規直接規範定義類如上述不請自來之大量電子郵件。但是，參考商業實務上，ISP業者依其與用戶間服務契約約定之定義，UCE係指：「依商業性廣告為主之電子郵件，包括未經對方同意，擅自寄發電子訊息至對方信箱者」(其中電子訊息係指「電子郵件、簡訊或其他經由通訊設備傳遞之資訊。」)[9]或「

[8] 黃菁甯，＜談未經邀約電子訊息法制國際趨勢與我國法制規劃＞，發表於台灣e產業法制環境研討會，2003 年 12 月 4 日

[9] **請參考附件一**--各ISP業者參加【ISP業者對濫發電子郵件之建議與期許座談會】之書面回應整理表

大量內容相同且為商業訴求廣告之郵件濫發電子郵件一詞」。[10]

三、本研究關於濫發電子郵件之工作定義

為便於本研究目的之實踐，本研究就上述不請自來之大量電子郵件，定名為濫發電子郵件，並賦予一個工作定義，以進行後續章節的討論。本工作定義對於濫發電子郵件的描述，包含以下數個或全部特徵：

(一) 濫發電子郵件通常是經過自動化機器產生而大量傳送；
(二) 濫發電子郵件發信人通常是匿名或掩飾其真實發信地址；
(三) 濫發電子郵件之發送對象為多數不特定收件者，甚至收件之電子郵件地址有時未必真實存在；
(四) 濫發電子郵件之發送通常未經各個收件者事前同意；
(五) 濫發電子郵件之訊息內容為商業性，不屬於政治、宗教、教育或文化目的者；
(六) 濫發電子郵件內容為虛偽不實甚或違法者；
(七) 濫發電子郵件往往沒有提供有效的回覆拒絕機制，使收件者可以拒收後續接踵而來的郵件[11]。

本研究報告後續展開之分析及討論，在未特別注釋及說明之情形使用濫發電子郵件一詞時，通常指具備以上(一)至(五)項描述特徵者；在介紹個別法規及司法判決例時，引用濫發電子郵件一詞則應依該節段所敘述法規及判決例之定義加以理解。

本報告未特別排斥對於濫發電子郵件指涉不法及虛偽不實內容之分析。因為，濫發電子郵件在網際網路的實像幾乎已經無法和上述具爭議性的內容分離看待處理；而本報告在最後一張結論與建議中述及濫發電子郵件一詞，在絕大多數情形兼納以上(一)至(七)項描述。

[10] **請參考附件一**--各ISP業者參加【ISP業者對濫發電子郵件之建議與期許座談會】之書面回應整理表

[11] 陳皓朋，＜打開spam，咀嚼沒有營養＞，PC Office雜誌，67 期，2003.2.，頁 80

貳、濫發電子郵件造成的影響

由於電子郵件具有「非同步溝通」、「快速傳送」、「支援文字、多媒體模式」、「一對多、一對一地溝通方式」、「外部性記憶」、「私密性」、和「指定、強迫回覆性」的特性，再加上技術進步、成本低廉和傳輸迅速等優點，已使得電子郵件成為一個強力的行銷溝通工具，然而大批傳送的濫發電子郵件卻是一般網路使用者和網際網路服務提供者的惡夢。

一、在網際網路企業使用者方面

依據美國網路業者美國線上（America Online）於 2003 年 4 月報告指出，依據其於 1999 年所裝置之軟體測出，到今日為止，依收件者指示加以過濾之濫發電子郵件量事實上佔全部郵件總量之一半。濫發電子郵件每日所發出的數量超過一百萬封，數量為 1999 年所測出數量之十倍[12]於美國自詡為反對濫發電子郵件軟體開發領導者之Brightmail 公司，宣稱該公司每半個月皆要為其客戶阻擋超過六億封濫發電子郵件。依據Brightmail公司之統計，該公司所過濾的郵件中有百分之四十八為濫發電子郵件，比 2001 年 4 月高出七個百分比[13]。

如洪水般湧進的濫發電子郵件已非僅可用擾人等字眼加以形容，濫發電子郵件不僅對收件者產生困擾，更重要的是收信者必須花費更多的時間去閱讀郵件的內容，並刪除這些擾人的郵件。根據統計，美國企業員工每天平均收到的濫發電子郵件約 13.3 封，每名員工每天平均要消耗 6.5 分鐘處理濫發電子郵件，若以每位員工每日薪資 30 美元，每月工作 22 個工作天為基礎計算，企業平均每名員工損耗 874 美元成本來處理濫發電子郵件，對於企業而言，濫發電子郵件已經不僅是對員工日常工作上造成干擾，在實質上更已造成相當龐大的損失。[14]

而依照美國電子商務研究公司 Ferris Research統計，這些

---

[12] See America Online, Inc. v. Maryland Internet Marketing, Inc., et al. U.S. District Court for the Eastern District Of Virginia, Civil Action No.03-469-A. http://legal.web.aol.com/decisions/dljunk/moorecomplaint.pdf

[13] *Id.*

[14] 楊正瑀，＜反垃圾郵件　政府、網路使用者皆有責任＞，Source週報，2003.8.11

擾人的電子郵件將使美國經濟於 2003 年損失超過一億元。[15] 另一個獨立研究機構Nucleus Research 於 2003 年 6 月研究報告亦作成相同之結論，依照該機構對於美國 76 個高科技產業之員工及管理階層所為之調查，認為濫發電子郵件使每個員工每年浪費平均美金 874 元之工作產能，或使每個員工工作產能下降百分之一點四 [16]。

更令人憂心的是濫發電子郵件所夾帶的電腦病毒，只要收件人接收，不需要開啟就受到感染，大量危害企業網路，附件網址亦可能附贈 Java or ActiveX 等惡性程式，許多特洛依木馬病毒（Trojan Horses）就是藉此大量擴散。

二、在網際網路服務業方面

鉅量的濫發電子郵件損壞電腦之儲存容量，也降低電腦間與線上文件儲存或運輸速度，迫使網路服務提供業者（ISP）必須花費數百萬元建置額外的電腦裝置或聘僱處理人員[17]來處理相關之問題。收件者及一般公司行號為阻擋濫發電子郵件，因此被迫購買過濾濫發電子郵件之軟體，但是因為濫發電子郵件發信人往往非常狡猾，這樣的軟體通常只能過濾部分的信件，有時候甚至會過濾到非不請自來的郵件。

我國國內ISP業者也表示，依據投資軟硬體設備，網路消耗頻寬及人力成本估算，平均處理每封濫發電子郵件成本約新台幣 0.02 元，每年約達新台幣 300-350 萬元。此成本包括頻寬、人力及系統軟硬體等成本，並僱請專責人員或成立SPAM處理小組(包含客服及系統管理等專職人員任務分組)。[18]

---

[15] See http://www.ferris.com/Welcome.html."Spam will cost U.S. organizations over $10 billion in 2003. For U.S.-based ISPs, 30% of inbound email is spam, while at U.S.-based corporate organizations, spam accounts for 15% to 20% of inbound email. Spam consumes computing resources email administrator and helpdesk personnel time, and reduces workers' productivity. Despite the increasing deployment of anti-spam services and technology, the number of spam messages, and their size, is continuing to increase rapidly."

[16] Based on findings that the average employee receives 13.3 spam messages and spends 6.5 minutes per day managing spam. See http://www.infoworld.com/article/03/07/01/HNspamcost_1.html.

[17] See *AOL v. IMS et al.*, U.S. District Court for the Eastern District of Virginia, Civil Action No.98-0011-A. http://legal.web.aol.com/decisions/dljunk/imsreport.html.

[18] ISP業者中華電信與和信多媒體代表於行政院經濟建設委員會財經法制協調服務法協中心（簡稱法協中心）與工商時報共同主辦「ISP業者對濫發電子郵件之建議與期許」座談會發言紀錄，2003 年 10 月 3 日.請參考 10 月 14 日工商時報

對於ISP業者而言，為了維持網路系統正常運作，必須加大頻寬、安裝新的過濾軟體程式以及撥用更大的容量以接收全部郵件，而這些花費最後勢必轉嫁到消費者身上，可能在未來造成消費者使用率的降低。除此之外，濫發電子郵件甚至成為阻礙網路發展的元兇，以台灣學術網路為例，濫發電子郵件的大量傳送，佔用網路頻寬成為網路塞車的最大禍首。[19]在網際網路上不斷變更路徑及發信郵件地址的濫發電子郵件，也引發了不同國家ISP業者之間窮於奔命，應付瞬間突增的網路流量。甚至，相互將對方伺服器位址列入黑名單，試圖阻擋多數不受歡迎的濫發電子郵件。如此一來，反而影響正當電子郵件的跨國傳送，影響正常交易進行。

目前我國的ISP業者以透過用戶契約約束方式，約定網路使用者無正當理由不得發送大量信件給其他用戶，如經發現則ISP業者將取消該用戶使用ISP業者所提供接取服務的權利，濫發電子郵件發信人為了掩飾其不當的違約行為往往都會使用假的電子郵件地址及利用其它人的郵件伺服器作為中繼(relay)來寄發廣告信。relay功能的出現，原先是為了方便接收郵件，使在遠端的一方可以藉由relay的功能在短時間內接收到郵件。但是濫發電子郵件猖獗，使得越來越多的郵件伺服器關閉relay功能，以阻擋濫發電子郵件的侵入。[20]

三、在網路使用者個人方面

對於網路使用者而言，不請自來的濫發電子郵件不但佔用收信人於網路伺服器中有限的硬碟空間，並造成收信人在下載此種濫發電子郵件個人時間、金錢上的損失。然而更令人擔憂的是，網路業者可能透過非法的手段蒐集或販賣資料，以取得個人電子郵件的地址，涉及侵害個人隱私權。對於提供網際網路接取服務的業者而言，由於大量內容重複的濫發電子郵件造成過度消耗公司的硬體資源，或者因瞬間寄發大量廣告信造成網路伺服器癱瘓以致於無法提供客戶服務。

---

[19] 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，81 期，2002.2.，頁 153

[20] 林宜隆，＜垃圾電子郵件之問題探討與管理因應＞，see available at: http://www.isecutech.com.tw/it_Feature_Content.asp?Serial_no=692，資訊安全科技網，2003.7.28（visited on 2003/9/10）

此外，任何使用網路之人都曾經收到濫發電子郵件，信件內容包括從簡易貸款、低利貸款之申請、色情的圖片、其他情色交易廣告或是藥品販賣。有時候非常難估算這些濫發電子郵件所造成的影響，當超過一半的郵件內容皆為如何容易賺錢或是提供色情圖片時，幾乎無從估計有多少人會因這些郵件而掉入廣告的陷阱。但是濫發電子郵件的發信人仍繼續散佈這樣的郵件。

以最近美國發生的案例來說明，在美國有人藉設立網站散佈大量郵件給他人，向收件人廣告，宣稱投資該公司將於一個月內可以有數十倍之利益回收，藉以詐欺收件人。他總共寄出了九百萬封的電子郵件，結果有二十九個人回覆，並匯入了超過十萬美元，也就是說，當送出超過三十萬封的電子郵件，就會有一個人成為受害者，而這樣的行為卻是日益猖獗，因為散佈郵件者送出一封信件之費用與送出一百萬封信件之費用是相同的。而依照現在已發生之案件觀之，美國已有好幾起發信人因為送出超過百萬封之濫發電子郵件，而被法院認定必須負起賠償責任。[21]

根據最新的報告顯示，網際網路上每年高達數十億封的濫發電子郵件，開始讓使用者對電子郵件通訊喪失信心。Pew Internet and American Life Project 的研究發現，有一半的網路使用者表示，濫發電子郵件已經讓他們越來越不相信全部的電子郵件；四分之一的人表示，因為濫發電子郵件而更少使用電子郵件。

這份在 2003 年 6 月間針對 1400 位網友所做的問卷顯示，大部份的人覺得面對濫發電子郵件覺得相當無力，無法防堵一些發財夢、藥品，及一些不想要的廣告每天寄進到自己的信箱。過半的人表示，濫發電子郵件的氾濫讓他們很難找到自己要的資訊。根據一些評估，濫發電子郵件目前大約佔去了所有電子郵件的一半，由於浪費頻寬和降低生產力而讓企業損失數十億美金。大部份的使用者表示，他們不會在網站上張貼自己的電子郵件地址以避免成為垃圾蟲收集的名單，其中許多人表示，會在工作場所或家裡使用過濾功能來防堵。

[21] See *AOL v. Forrest Dayton*, U.S. District Court for the Eastern District of Virginia, Case No.98-1815-A. http://legal.web.aol.com/decisions/dljunk/dayton.html ; See *AOL v. CN Productions* (E.D. Va. 2002),U.S. District Court for the Eastern District of Virginia. http://legal.web.aol.com/decisions/dljunk/cnproductions12-2002.pdf

但也有部份使用者也承認，曾有過助長這些問題的行為。7%的人表示，曾經購買濫發電子郵件裡的產品與服務，三分之一的使用者表示，他們曾經因為想進一步知道更多訊息而點選裡面的連結。三分之二的人表示，曾經點選濫發電子郵件裡「取消訂閱」的連結——然而此舉只會產生更多濫發電子郵件。[22]

參、管理濫發電子郵件的可行機制

我們熟知的網際網路是建立在網路上不同電腦間的通訊協定(Internet protocol,簡稱 IP) ，這一套系統能夠運作基本上需要兩種位元資料，一邊是送出訊息的電腦 IP 位址所在，另一邊就是訊息將送達的電腦位址。訊息來回在不同的電腦位址間傳遞，不會顯示出發信人，收信人或甚至是傳遞過程中接觸到這些資料所有的網際網路使用者個別有關的身分資訊，唯一能夠識別到的只有類似 128.34.25.508 這樣的一組阿拉伯數字。如此設計，我們知道是為了儘量簡單化，以便在核子戰爭的灰燼中快速回復通訊聯繫，但是後來的發展卻有趣地排除了複雜的控制設計，促成一個自由的”想像空間”出現。 在網際網路基本通訊協定之下出入網際網路的行為，可以被網路伺服器紀錄到的只有行為人位於網際網路上的 IP 位址，以及他是以與網際網路通訊協定相容的方式登入網路。這就像你要進到一個大型的主題樂園遊玩，必須先買門票，進入之後不同的設施有不同的使用者限制及玩法規定，甚至要再一次接受檢查身分年齡與身體狀況；但就在主題樂園旁邊一個開放的海灘，不需入場券，沒有遊戲規則，也不必隨時接受檢查身分，你可以隨時來隨時去，同場玩樂的其他人也不會知道你是誰以及你來自何處。“匿名”或 ”匿蹤”成為網際網路的優勢，也是它的致命吸引力。 “匿名”是網際網路受到大眾熱烈喜愛的因素之一。 可以隨時來去，不必擔心別人知道我是誰，游逸於不同的角色扮演，為網際網路使用者在真實空間裡開闢出一道任意門，通向所謂的虛擬空間(或網路空間) 。事實上，它不只一個，而是成多數狀態並存於真實空間，卻能讓大眾以非同步方式利用，這帶來驚人的時間轉移效果以及場所轉移效應—公司職員早上九點不到就已經在辦公桌前就定位，勤奮地以電腦連上網際網路處理事務:接收公務電子郵件，同時打開不同視窗為

[22] CNET新聞專區，＜研究：垃圾郵件阻礙e-mail使用意願＞，2003.10.24.

私人的投資組合看盤下單，順便為女朋友瀏覽購物網站的精品拍賣出價。網路空間這麼大規模的社會聚落，沒有時間差別，沒有地域距離限制，最重要的是每個進場者都興致勃勃，躍躍欲試從來不曾在表示自我身分情形下膽敢嘗試的事情，當然商機也因緣際會在此生根。一九九四年起，網際網路上的商業應用接二連三興起，距離一九九一年美國國家科學基金會(National Science Foundation) 允許網際網路使用在商業活動上還不到三年，接下來發生的事情則是所有網路使用者都親身經歷了那一波又一波快速拉起復劇烈震盪的築夢狂潮，至今還未歇息。然而，網路空間原來所吸引人的"匿名"環境卻是迄今飽受批評，在政府和商業界的雙管壓力之下面臨根本性的改變，來去掉這一個原生的特質。濫發電子郵件現象，更是進一步激化了改變的步調與幅度。目前全世界對於管理濫發電子郵件已經採行之防制機制可分為科技、市場及法律三種解決方式，茲分述如下：

一、科技的解決方式

2003 年 11 月 24 日出版的美國新聞周刊雜誌(Newsweek)將全球科技界對抗濫發電子郵件總動員形容為一場保衛電子郵件收件匣的戰鬥(Spam Wars: The Battle for the In Box) 。

實務上 ISP 業者解決或減少濫發電子郵件數量的做法，以採用過濾信件（filtering）程式的方式最為常見，設計執行過濾程式的功能一般會考量以下三種面向：

（一）自發式過濾（Heuristic Filtering）

又可分為兩種不同之做法：

1. 自源頭進行之自發式過濾(Origin-Based Heuristic Filtering)：
   即針對可能是濫發電子郵件發信人之發信 IP 位址預先建檔，對所有發出自該位址的郵件進行攔截和過濾。

2. 自訊息內容進行之自發式過濾（Message-Based Heuristic Filtering）：
   以訊息之內容屬性區分，利用過濾程式篩選可能的濫發電子郵件。

（二）合作式過濾（Cooperative Filtering）

同時採取下列兩種做法或擇取其中一種：

1.收件者登記（Recipient registration）

收件者向 ISP 業者或其他中介機構登記，以表明其願意接收或拒絕接收濫發電子郵件。

2.發信人標示（Originator labeling）[23]

由發信人於發出的郵件標題主動標示這是屬於大量寄發或具有商業性質之電子郵件。

（三）經收件者事前同意或事後拒絕

1.事前同意（Opt-in，又稱為選擇列入）：

經收件者同意才能寄發電子郵件，非經同意不得對之寄發電子郵件。

2.事後拒絕（Opt-out，又稱為選擇取消）：

收件者如不想再收到電子廣告郵件，則可要求發信人將收件者列入取消發送名單，故又稱為選擇取消。

採用過濾程式來阻擋濫發電子郵件也許仍稱不上是最完美的解決方案，尤其使用俗稱黑名單(Blacklists)過濾軟體程式最大的缺點在於往往會將收件者一般非濫發的電子郵件也阻擋在外，無法接收進來。因此各項改進的技術不斷推陳出新，包括：

（一）許可清單（Whitelists）

目前微軟公司（Microsoft Inc.）已計畫在 Hotmail 免費郵件服務當中，採用許可清單（Whitelists）的方式，阻擋濫發電子郵件。微軟對旗下 Hotmail 服務的使用者發出通告，表示將全面升級 Hotmail 系統，加入許可清單功能，依該公司預告這一項新服務的原理，是利用使用者自己建立的郵件地址清單，來過濾所有對使用者發送的郵件。只要該郵件地址不在許可清單當中，使用者的個人信箱就不會真的收到該郵件。許可清單因此被視為對抗濫發電子郵件的各種科技方案當中，最為嚴格的一種（黑名單則是阻擋

[23] 詳見王郁琦、陳炳全，前揭文，頁 157 以下

在郵件地址清單當中的郵件）。

在Hotmail的做法當中，如果收到的電子郵件發自許可清單所列電子郵件地址，這些郵件就會列在每個使用者登錄時所見到的今天（Today）首頁。在微軟預告的解說當中指出，「你的連線將從今天首頁開始，在首頁當中你也只會看到你認識的人所寄來的郵件。滿足『認識』的條件，需要發信人的郵件地址在你的許可清單當中，所以你只會先看到對你重要的郵件。」Hotmail的使用者，隨後可以點選「郵件」檔案匣，顯示所有的收件匣。Hotmail也提供了「垃圾郵件」的檔案匣，儲存Hotmail系統認為是垃圾郵件的郵件。

因為濫發電子郵件的增加和及其所造成的成本，促成防治和管理濫發電子郵件的新市場。微軟新服務的預告，緊接在雅虎發表新的濫發電子郵件防治功能之後。雅虎提供使用者在網路上訂閱其他服務時的假造郵件地址功能。微軟發表新服務的動作和美國國會通過 CAN SPAM ACT 2003 法案同一天，該法案也要求政府專責機關建立全國拒絕濫發電子郵件的使用者名單。

Hotmail 除了許可清單的功能，也簡化了使用者提報濫發電子郵件的方式。Hotmail 的升級版功能會顯示，在收件匣當中的郵件，是否來自收件者的通訊錄所輯錄電子郵件地址。Hotmail 在其最新的版本中，亦提供了所謂「圖像過濾器」來防止使用者的電子郵件地址被蒐集。其方法乃是藉由收件者在下載信件上附加的圖像時，會先封鎖郵件中的影像，並提醒收件者是否真要下載，以防止網路上不法人士在郵件圖像中隱藏的蒐集帳號、郵件程式被使用者下載，並導致其電子郵件地址曝光，從此遭受濫發電子郵件轟炸之後果。微軟並承諾將在近期更新行事曆和通訊錄的應用程式。

EarthLink 和 America Online 等 ISP 業者作為微軟主要的競爭對手則表示，在他們現有的服務當中，早就已經有許可清單的功能。 AOL 的發言人指出，「濫發電子郵件是整個產業的問題，我們很高興看到微軟推出我們去年就已經推出的濫發電子郵件防治服務。」

AOL表示，在 2002 年秋天的時候，AOL就引進了「已知聯絡住址（known contacts）」的郵件選項，AOL並且在 2003 年 6 月推出依照「已知聯絡住址」排列郵件的功能。[24]

（二）傳輸協定之整合

有鑑於目前防堵濫發電子郵件的方法各不相同，反濫發電子郵件研究小組（ASRG-- Anti-Spam Research Group）將努力整合不同的技術，藉某種呼叫者身分確認電子郵件的來源。隸屬於網際網路研究任務小組（IRTF--The Internet Research Task Force）的 ASRG 10 月成立小組委員會，希望化解各種傳輸協定（protocol）之間的歧異。這些協定的共同作用是：確認傳送電子郵件者和郵件上載明的發信者身份吻合。

但若依照簡單郵遞傳輸協定（SMTP）現在的運作方式，目前並無一種普遍通行的方法可做那種確認。這導致一些人建議修改 SMTP，或乾脆把這種通用的協定給撤換掉。許多人提出在不廢除 SMTP 的情況下進行電子郵件確認的建議方案，其中不少提案已呈交 IRTF 審查。IRTF 是網際網路技術任務小組（IETF—The Internet Engineering Task Force）的關係組織。

目前已浮上檯面的建議技術包括：獲准發信人來源（Sender Permitted From，簡稱 SPF）、指定發信人協定（Designated Mailers Protocol，簡稱 DMP）和逆向郵件交換（Reverse Mail Exchange，簡稱 RMX）。ASRG 新成立的小組委員會負責把這些技術融合成單一的技術標準。

這些相關技術背後的概念，是修改網域名稱系統（DNS）資料庫，好讓電子郵件伺服器能公布郵件發信源的網際網路位址（IP），那麼 ISP 業者在接收電子郵件的同時，即可確認那封電子郵件的來源是否名實相符。

這套系統可保護電子郵件伺服器和個別的電郵帳號所有

[24] 黃晨哲，＜Hotmail新制力抗垃圾郵件＞，CNET新聞專區，2003.10.24

人，讓他們的電子郵件地址不被他人冒用，而被懷疑成濫發郵件者。已有一些方法設法解決此問題，例如「可信賴電子郵件開放標準」(Trusted E-mail Open Standard)。但是到目前為止，這些方法都尚未獲得廣泛採用。

ISP 業者和反濫發電子郵件問題專家都表示，冒用他人電子郵件的發信電子郵件地址，是遏止濫發郵件的根本障礙。濫發郵件者通常藉入侵保護不周的電子郵件伺服器、挾持其他電子郵件伺服器、偽造姓名及電子郵件寄信欄住址等方法隱匿行跡。

ASRG 成員對小組委員會推動以統一協定解決濫發電子郵件的問題表示樂觀，希望能以此法取代立法規範，或強迫使用者按傳發郵件則數付費的解決辦法。

「我們可用技術解決濫發電子郵件問題，不必國會立法干預，或強制執行小額計費制，」ASRG成員暨費城電子郵件服務商Pobox.com創辦人兼技術長Meng Wong說。Pobox.com今年稍早估計，該公司處理的電子郵件當中，70%以上是濫發電子郵件。Meng Wong說，發信人身分確認系統必須搭配某些類型的信譽評價系統，藉此協助收件者辨認已知濫發者的網域名稱。「網域名稱無法造假，一旦信譽評價系統揪出問題的網域名稱，那麼不論濫發郵件者侵入多少部機器，用的還是濫發者的網域名稱，那麼我們就逮得到他了。」[25]

（三）可拋式電子郵件地址（disposable email address）

可拋式電子郵件地址為雅虎（Yahoo！）推出對抗濫發電子郵件的方法之一，所謂可拋式的郵件地址，就是使用者可在一個長期有效的郵件地址上，自行訂定一個變化的帳號名稱以及郵件地址的使用期限，過了期限後，這個經個人變化過的郵址就不再有效，濫發電子郵件就會減少。可拋式電子郵件地址可使用的場合包括，有必要填郵件地址、卻不想讓對方長期騷擾，以及只需要短期內聯絡等情況。例如使用者在需要於網路上公開其電子

[25] 唐慧文，＜反垃圾郵件協定邁向整合＞，CNET新聞專區，2003.10.28

郵件地址的場合，即可使用一個另外編造、變化過的郵件地址，使得這些有期限性的資訊或是濫發電子郵件者將信件寄到這個信箱來，一旦使用者發現該信箱內容已被濫發電子郵件充斥，或是不再需要這些有時效性的資訊時，即可再變換成另一個電子郵件地址，或是將該電子郵件地址取消[26]。

（四）收件端的軟體過濾程式

對於何謂濫發電子郵件之認定，由於每個人對於濫發電子郵件的定義不同，因此無論法規規範如何完善、ISP 業者的郵件過濾器功能如何強大，通常還須等到收件者親自看過郵件內容後，才能對這封信件是否屬於濫發電子郵件下一個定論。職是之故，如何能在收件端阻攔濫發電子郵件，對於對抗濫發電子郵件問題可謂形成了最後一道防線。

目前，在收件端具有過濾濫發電子郵件的程式軟體，包括了微軟的 Outlook 2003 及趨勢軟體的 SPS（Spam Prevention Service）垃圾郵件防治服務等。微軟應用在 Outlook 2003 之過濾濫發電子郵件技術，包括：

1.可信賴的發信者清單：

使用者享有定義濫發電子郵件之控制權，其可選擇只接收從通訊錄中已設定的收件者或特定的電子郵件地址中收取信件，或僅從特定之領域中收取。

2.真人互動證明（Human Interactive Proofs，HIP）：

此技術是藉由在新 Hotmail 和 Passport 帳號的登記流程中使用的技術。這個技術可以確保這些登入的帳號是由個人所製作的，而不是由電腦或自動化產生的大批帳號中的一部份，以防止濫發電子郵件者利用電腦或自動化產生的大批帳號登入，並藉此寄發大量垃圾信件。此技術的方法為，在帳號登入的畫面上顯示一個隨機產生的畫面或文字，並要求登入者填入這個畫面或文字中的內

[26] See http://news.com.com/2100-1038-5094171.html （visited on 2003/10/22）

容，因此登入者必須是真人操作，而無法以電腦自動登入來代替。

3.機器自動學習（Machine Learning）：

這個技術為藉由軟體中濫發電子郵件的組合管理，讓使用者自行定義其濫發電子郵件組合管理之層級，以及選取濫發電子郵件處理方式。經過一段時間之後，過濾器會從使用者選擇的方式中訓練辨識何種信件為濫發電子信件，並學習其辨識之標準和能力，以在日後更加準確地偵測並排除濫發電子郵件的進入。

而在趨勢科技的 SPS（Spam Prevention Service）垃圾郵件防治服務方面，該服務為一可獨立執行於 Windows、Solaris 和 Linux 平臺之軟體，其運作方式將整合於閘道端郵件防毒與內容安全伺服器（InterScan Messaging Security Suite，IMSS）中，介於防火牆和企業資訊系統之間。

其採用的「智慧型啟發式 Heuristic 技術」，是根據郵件中的多項特徵值（如：mail header,SMTP envelope, MIME...）進行交叉計算所得出的一組機率值，作為判定這封郵件是否為濫發電子郵件之依據。若郵件被判定為濫發電子信件後，會被標記後傳送到一個預先設定的信箱，而該軟體中則會保存完整的收信紀錄，並提供基本的管理報表，俾使收件端能對郵件作有效的管理。

該軟體的特色之一，是可將阻絕濫發電子郵件任務和防毒及內容安全解決方案結合，有效防制混合型濫發電子郵件之威脅，降低電腦系統負擔及生產力的損失。

除此之外，目前技術面可行之過濾方式尚有下列數種，茲列表如下：

【表 2.1 垃圾郵件過濾方式一覽表[27]】

過濾方式	軟體公司	產品名稱
1.以郵件特徵判定	Brightmail Cloudmark SurfControl	Anti-Spam Authority E-mail Filter
2.由全體使用者「投票」決定	Cloudmark	ApamNet
3.建立網絡式過濾閘道，在信件進入電腦前先行過濾攔截	Computer Associates CipherTrust NetIQ IntelliReach	Etrust IronMail PureMessage MailMarshal Message Screen
4.經由不斷嘗試錯誤，或根據一定規則，篩掉具有濫發電子郵件特徵的信	McAfee Security SpamAssassin Elron Software Matterform	SpamKiller Open-Source software Message Inspector SpamFire
5.具學習力，紀錄使用者刪除郵件的特徵，以這些特徵過濾郵件	Microsoft Spammunition	MSN 8.0 Freeware
6.只接收「許可」名單寄來的郵件	Habeas AOL	Sender Warranted E-mail Whitelist feature
7.如接種疫苗般，將使用者的電子郵件地址隱藏起來，不被 spammer 發現	Matterform Sneakemail	Spam Vaccine Sneakemail

綜上所述，目前技術上解決濫發電子郵件的方式仍以過濾郵件技術為主。由於網路使用者對於減少濫發電子郵件之需求殷切

[27] 巫姿惠，＜打擊SPAM總動員＞，HOPENET科技月刊，創刊號，2003 年 10 月，頁 69

，故各 ISP 業者、軟體開發公司無不傾全力開發，試圖減少濫發電子郵件所造成之問題，並已獲致一定之成果。然而，追究濫發電子郵件氾濫之原因，可知問題之產生實由於電子郵件之便利性與費用低廉，且將成本轉嫁至 ISP 業者及收件者，以致濫發電子郵件所花費之成本與所獲致之可能利益相比，足令發信人願意發展反過濾技術，或冒被過濾攔截的風險，以求達成濫發電子郵件之目的；更有甚者，以技術過濾的結果，由於成本低廉，反而可能促使濫發電子郵件發信人蒐集更多的電子郵件名單，以求達到其行銷等商業性之效果。

接受本研究訪談之我國ISP業者則異口同聲表示，技術只能解決部份濫發電子郵件帶來的問題，其建議需要有相關法律條文的強制管制及政府專責的處理單位介入才會更有功效。[28]

二、市場的解決方式

所謂市場的解決方式，係指藉由市場力量供需法則，減少濫發電子郵件之經濟上誘因，或增加濫發電子郵件發信成本等，以期根本杜絕藉由電子郵件作為行銷管道所衍生之惡質問題。本研究歸納市場的解決方式有下列六項：

(一)提高使用電子郵件成本：

> 由於濫發電子郵件的產生導因於發信人的寄信成本過低，並且將成本不當地轉嫁到收信者的身上，故有謂如果將寄信成本提高，將可以減少濫發電子郵件的產生。但是，採行此種方式將會間接提高網路上的溝通成本，而徹底地改變網路溝通模式，利用電子郵件進行通訊的優點將不復存在。[29]

(二)依願意收取濫發電子郵件分級付費：

> 搭配上述增加發信人電子郵件發送成本的想法，相對在收件者方面，仿效有線電視收視分級付費制度，建立網路上

[28] **請參見附件一**---各ISP業者參加【ISP業者對濫發電子郵件之建議與期許座談會】之書面回應整理表

[29] 詳見王郁琦、陳炳全，前揭文，頁 159

收閱濫發電子郵件分級付費制度，使表明願意接收濫發電子郵件者，所需支付的網路使用費用低於表明不願接收者，如此既可使電子郵件使用者得以依其需求，選擇網路接取服務使用費率之高低，並可兼顧廣告主之行銷需求。

(三)採行以價制量原則：

同樣是搭配上述增加發信人電子郵件發送成本的想法，對於電子郵件的發送，以量計價並採累進費率，寄發越多電子郵件者，則應負擔更高費用，這個構想同樣必須建立在寄發電子郵件應付費之概念。

(四)「電子郵票」(e-stamp)：

我國知名的經濟學者施俊吉認為，目前解決濫發電子郵件的策略有二種，一是「阻擋」，另一是「強迫減量」。就「阻擋」而言，手段是「過濾」，惟過濾郵件的內容不免侵犯個人隱私，所以阻擋策略成效有限，且爭議不斷。阻擋策略既難奏效，「強迫減量」之對策或可一試。其提出試行「電子郵票」(e-stamp)之機制：1、有電子郵票，才能寄電子郵件；2、電子郵票可以重複使用，收件者回信時准用來信之郵票。

電子郵票一旦實行，濫發電子郵件便需付費。一般常情，收到濫發電子郵件的人是不會回信給濫發電子郵件的製造者，所以電子郵票便一去不回，形成發信人真正的成本負擔。只要發電子郵件的行銷方式不再經濟免費，濫發電子郵件當然減量，至於正當的網路通訊者，由於雙向通信可以重複使用同一張電子郵票，負擔自然有限。如此方策，既能打擊濫發電子郵件的製造源，又不致傷害正常的通訊活動。[30]

美國波士頓的網路自由作家Robert Hettinga亦舉例說，若由ISP業者共同訂出標準，將每寄一封信以 0.1 分美元的價格計算，這樣的收費方式對一般用戶並不會造成顯著效果，但對於發信數量動輒數萬封的spammer而言，這樣的做法將可以讓他們知難而退。[31]

[30] 施俊吉，＜垃圾郵件＞，中國時報，B1 版，2003.10.2.
[31] 巫姿惠，前揭文，頁 69

（五）計算機計費技術：

還有一種類似於寄信貼郵票的方式，但不是以金錢當寄件的交換對價，而是從電腦微處理器的設計下手。電腦系統將被設定為每寄發一封郵件，便自動停滯幾秒鐘的時間，這招用在濫發電子郵件發信人身上，將會使他們賴以發信的微處理器遭到嚴重損害，目前微軟的研究單位，和以 Open-source 方式運作的 Camram 公司皆已著手開發這種稱為「計算機費用」的技術。

（六）透過寄送郵件授權以量定價：

一個名為 The World's Shien 的團體提出建議，他們認為應該促進網路上的市場秩序，由合法的 ISP 業者來組成「電子郵件付費清算中心」(e-mail cleaninghouse)，這個組織提供具有認證密碼的授權給合法正當但需大量發送電子郵件的人，而授權的價格就依照所發送的郵件數量來計算(好比是收取版稅的方式)。[32]

但是，市場的解決方式未必是受到歡迎的解決方案。本研究所訪談立場上支持嚴格管制濫發電子郵件運動者，全數反對犧牲網際網路免費利用自由，卻是換取少數的 ISP 業者坐享豐厚的市場利潤。其中，例如 The Spamhaus Project 總幹事 Steve Linford 就強調，全球反制濫發電子郵件立法應置重在禁絕(banning) ，而非對濫發電子郵件合法化及正當化後，再加以管理(regulating) 。即便是受訪的 ISP 業者代表對於向電子郵件發信人採行收費機制，以價制量也難青睞。美國雅虎總公司負責國際公共政策事務的部門負責人 Dr.Stephen Collins 也認為，網際網路最偉大也是最吸引人之處就在於它是免費的；透過對大量發送郵件者收費，未必能有效減少濫發電子郵件的數量。他補充道，雅虎目前對其控管的郵件伺服器設定了，每個電子郵件地址每次能發送電子郵件數量以二十五或三十件為限。

[32] 巫姿惠，同前註

三、法律的解決方式

（一）ISP 業者與用戶間的契約

ISP業者在私法自治原則下，以其與用戶間的使用服務契約約定，建構起反制濫發電子郵件發信人的防線，透過各個適用的法規賦予上述契約約款強制執行的效果，並在主管機關的監督下，各個ISP業者協力統合一致的行動方案，包括加強交流對濫發電子郵件發信人活動蹤跡的通報，聯合採取共同封鎖措施，都是可能的較佳解決方法。我國交通部電信總局已於網際網路接取服務相關定型化契約範本內明定禁止濫發廣告郵件之約定條款[33]，提供ISP業者共通的行為準則以及對抗濫發電子郵件發信人法律依據；[34]本研究整理我國主要ISP業者相關反制濫發電子郵件之契約內容如表 2.3，供作參考。

本研究訪談我國主要 ISP 業者，深探以 ISP 業者與用戶間的契約作為管制濫發電子郵件的手段實施成果發現，受訪 ISP 業者普遍反映此手段之有限性，無法有效減少濫發電子郵件氾濫現象：35

- -使用服務契約約定僅能消極停止對濫發電子郵件用戶提供服務無從積極防免；
- -契約約定欠缺如實定法之強制性；
- -依契約約定就個案提起民事訴訟追訴之成本與可能獲得之賠償金額懸殊顯不相當；
- -契約約定之實際嚇阻效果極微；
- -業者無從追查濫發電子郵件發信人真實身分。

上述調查結果進一步披露，ISP 業者多數主張，應以政府公權力介入，立法管制濫發電子郵件。

---

[33] **請參見附件二**---交通部電信總局「撥接連線網際網路接取服務定型化契約書範本」

[34] 交通部電信總局「撥接連線網際網路接取服務定型化契約書範本」第十九條（禁止濫發廣告郵件）約定：「甲乙雙方均不得於網路上以任何方式發送未請求之廣告郵件。
一方發現他方發送未經請求之廣告郵件情事時，得採取下列措施：
（一）、要求他方立即停止發送。
（二）、如他方未能於適當期間內（不超過____星期）回覆，
任何一方有權終止承租人契約。」

[35] 中華電信代表於行政院經濟建設委員會財經法制協調服務法協中心（簡稱法協中心）與工商時報共同主辦「ISP業者對濫發電子郵件之建議與期許」座談會發言紀錄，2003/10/3.。請參考 10 月 14 日工商時報.

（二）政府立法管制

以政府公權力介入，立法管制濫發電子郵件之正當性何在？以傳統垃圾郵件與濫發電子郵件比較，傳統垃圾郵件之寄送尚無以立法管制之實例立法委員馮定國分析相較於傳統垃圾郵件，濫發電子郵件之發信者發信成本低廉，且轉嫁至 ISP 業者及收信者，由其負擔收受濫發電子郵件之外部成本，形成類似環境污染之外部性，因此管制濫發電子郵件較傳統垃圾郵件具有更高之正當性(參見表 2.2)。

世界各國已見對於濫發電子郵件立法管制之成例，除了美國在其憲法第一條修正條文就商業性言論之適用容或有爭議之外，其他各國對於相關立法之正當性，尚無疑問。進一步即應探究，以法律強制規定進行對濫發電子郵件行為管制可行的基礎架構為何。本報告第三章詳細整理國際管制濫發電子郵件之規範，並分別論述主要的兩種方案：事前同意機制(Opt-in)與事後拒絕機制(Opt-out) 。

【表 2.2　傳統垃圾郵件與電子垃圾郵件之比較[36]】

	製作費用	郵寄費用	收件人費用	結論
傳統垃圾郵件。	由寄件公司承擔，印刷成本高。	郵費由寄件公司承擔。大量寄送時費用也增大。	無。	發信人負擔所有費用。
電子垃圾郵件。	由寄件公司負擔，幾乎沒有成本。	以網路傳送，幾乎沒有成本，可一次寄發給百萬人。	收件人必須負擔上網之費用，包括網路公司服務費，撥接收信之電話費，以及連線閱讀時之電話費。	收信人負擔幾乎所有費用，網路服務業者（ISP）之連外頻寬亦遭佔用，所有用戶之上網服務品質也受影響。

[36] 立法院議案關係文書，院總第一七七七號，委員提案第三〇〇四號，立法說明

【表 2.3　我國主要 ISP 業者規範濫發電子郵件之定型化契約】

ISP 業者	契約或規範名稱	定型化契約中有關濫發電子郵件相關之規定內容	路徑
中華電信股份有限公司(HINET)。	HiNet 客戶規範。	在「網頁郵件系統」中之"客戶規範"有特別在第八條說明： "客戶不得於網路上用任何方式發送大量郵件，以避免浪費網路資源及加重本公司系統之負擔。若客戶發送大量郵件，一經本公司查證屬實，本公司有權終止該客戶之使用並於網站上公佈其帳號。"此外"違反規範用戶名單之用戶因發廣告信依據上列處理原則給予停止上網。"的說明,並列有違反規範名單"	http://www.hinet.net/footer_rule.htm
台灣電訊股份有限公司。	iSpeed (極速網)寬頻服務用戶約定條款。	在「iSpeed (極速網)寬頻服務用戶約定條款」第 20 條有說明: "用戶須遵守全球網際網路使用規則並遵循 Internet 國際應用慣例及網路禮儀，包括但不限於下列規定： I. 嚴禁於網路上從事違法行為。 II.嚴禁傳播具威脅、色情或破壞社會善良風俗之資訊或圖片。 III.嚴禁發送任何未經收件人同意之廣告郵件。 V.嚴禁散播電腦病毒、干擾通訊、破壞網際網路系統或破壞、擷取他人資料之行為。 V.嚴禁侵害他人商標權、著作權、營業秘密或其他智慧財產權。會公布黑名單。	http://www.ttn.com.tw/ispeed/online/
和信超媒體股份有限公司(GIGA)	Giga Mail 電子信箱(含無毒信箱)使用條款（公佈日期：2003.2.15）	在「Giga Mail 電子信箱(含無毒信箱)使用條款」第四條，使用者行為中項目中： 您不得經由本服務於網路上用任何方式發送大量電子郵件，或未經收信人同意收發、傳送廣告信函，以避免浪費整體網路資源及加重本公司網路系統之負擔。您如發送之大量郵件，本公司有權立即終止您之e-mail使用權限。您應定期收取電子郵件並閱後自行備份而後刪除，本公司不負儲存郵件之責。如您之郵件空	http://mail.gigigaga.com/

		間超過約定之容量、本公司有權不經通知刪除超出容量部分之郵件，並得視情節輕重終止您使用e-mail空間之權限及您的會員資格。	
亞太線上服務股份有限公司(APOL)	亞太線上廣告信處理辦法	亞太線上廣告信處理辦法為專文專款說明— ■ 公告對象： 亞太線上（以下稱本公司）專線用戶、Co-Location 用戶、Mail Hosting 用戶、ADSL 固定制用戶、ADSL 非固定制用戶、56k 撥接用戶、Cable Modem 寬頻上網用戶、VDSL 寬頻網路用戶、AVS 寬頻網路用戶 ■ 公告內容： 本公司針對以上用戶大量發送廣告信所採取之處理辦法及相關問題說明。 ■ 公告事項： 一、處理依據: 本公司於各網際網路服務契約中皆已明定用戶不得於網路上用任何方式寄送大量郵件，且本公司對於違反條款者亦有權不經用戶同意而停止其使用權。適用對象之服務契約連結如下： 亞太線上服務股份有限公司用戶相關服務營業規章 二、處理方式: 為避免影響本公司其他用戶權益，擅自寄發大量廣告信者，本公司將依照規章暫停貴公司或用戶之該帳號使用權，並公告於違反規範用戶名單網頁。 ■ 停權方式如下： 一、本公司網路使用者未經對方同意，擅自寄發大量郵件或廣告信至對方信箱：針對未經對方同意，擅自寄發廣告信至對方信箱者(Spammer 廣告信寄發者)，如經他人檢舉貴公司或用戶擅自寄發廣告信二次以上(含二次)者，本公司將暫時擱阻貴公司或用戶所有 IP 網段之發信功能，直至貴公司或用戶處理完成為止。貴公司或用戶若未改善而遭他人再次檢舉擅自寄	http://activity.apol.com.tw/notice/spam.html

		發廣告信者，本公司得暫停其帳號之使用權(停權方式：第一次十四日、第二次三個月、第三次六個月)，並公告於違反規範用戶名單網頁，其並應自負一切法律責任，停權期間使用者仍應繳交各項費用。 二、本公司網路使用者 E-mail 主機因未關閉 Open Relay，而被他人利用來發送廣告郵件：自本公司第一次給予警告日起三日後，貴公司或用戶若未改善而遭他人再次檢舉擅自寄發廣告信或未關閉 Open Relay 者，本公司得暫停其帳號之使用權(停權方式：第一次十四日、第二次三個月、第三次六個月)，並公告於違反規範用戶名單網頁，其並應自負一切法律責任，停權期間使用者仍應繳交各項費用。 三、被檢舉客戶申訴：如用戶於被停權期間已有效改善或處理完畢，可向本公司提出申請恢復使用權，申請方式請使用service@apol.com.tw信箱或撥本公司客服專線 0809-058-999。 四、相關問題： 1. 關閉Open Relay功能，可參考 http://mail-abuse.org/tsi/ar-fix.html，或請相關設備廠商協助。 2. Spam Mail 常見問題可參考網址 http://spam.gsnmm.gov.tw/。 五、檢舉信函經查證如有誣陷他人或竄改郵件標頭之事實者，本公司將依法移送有關單位處理。 六、本公司非常重視廣告信件濫發的問題，以後只要是您的信箱有收到本公司用戶所發的廣告信，您可附上完整信件『標頭及內容』轉寄至 spam@apol.com.tw即可，這是專責受理此項問題的信箱。 *如何附上完整信件『標頭及內容』？ 1.如果您使用 Netscape 傳訊者：檢視(V)-> 顯示標頭(D)-> 所	

		有資訊(A) 然後將該封信轉寄(Forward)。 2. 如果您使用 Outlook Express：該封信件標題上按右鍵，選「以附加檔案方式」轉寄。 七、若是您檢舉的廣告信並非本公司管轄網域所發出，本公司並無權對非本網域所發出的IP做任何查核或處分的作業，麻煩請將該信件轉寄給適當的網路管理者。(請參考他家ISP業者之廣告信檢舉信箱) 八、若您對本公司所提供之服務有任何建議或申訴，歡迎批評、指教，並請註明您的姓名及聯絡電話。申訴方式亦可使用service@apol.com.tw信箱或撥本公司客服專線0809-058-999。	
雅虎國際資訊股份有限公司(YAHOO)	Yahoo!奇摩服務條款	在「Yahoo!奇摩服務條款」第七條使用者的守法義務及承諾： 您承諾絕不為任何非法目的或以任何非法方式使用Yahoo!奇摩，並承諾遵守中華民國相關法規及一切使用網際網路之國際慣例。您若係中華民國以外之使用者，並同意遵守所屬國家或地域之法令。您同意並保證不得利用本服務從事侵害他人權益或違法之行為，包括但不限於： A.公布或傳送任何誹謗、侮辱、具威脅性、攻擊性、不雅、猥褻、不實、違反公共秩序或善良風俗或其他不法之文字、圖片或任何形式的檔案於Yahoo!奇摩上； B.侵害他人名譽、隱私權、營業秘密、商標權、著作權、專利權、其他智慧財產權及其他權利； C.違反依法律或契約所應負之保密義務； D.冒用他人名義使用本服務。 E.傳輸或散佈電腦病毒； F.從事不法交易行為或張貼虛假不實、引人犯罪之訊息； G.販賣槍枝、毒品、禁藥、盜版軟體或其他違禁物； H.提供賭博資訊或以任何方式引誘他人參與賭博； I.濫發廣告郵件；	http://tw.yahoo.com/info/utos.html

		J.其他 Yahoo!奇摩有正當理由認為不適當之行為。	
數位聯合電信股份有限公司(SEEDNET)	ADSL 租用條例	在 ADSL 租用條例之「共通條款」第 10 條： --用戶應遵守網際網路國際使用慣例，不得有入侵網際網路上其他系統之意圖與行為；不得破壞網路上各項服務亦不得在網際網路上以任何方式發送大量郵件造成本公司系統之障礙或從事違反公共秩序、善良風俗、及法律所禁止之行為。如有違反，除須自行負責外，本公司為維護服務品質，依網際網路國際應用慣例，得終止用戶之租用，任何後果及可能損失概由用戶自行承擔。用戶不得於網路上用任何方式執行本公司郵遞主機上所列服務項目以外之任何程式，用戶違反規定造成本公司損失者，應負賠償責任。	http://adslonline.seed.net.tw/index.asp

第三章　國際管制濫發電子郵件之規範研究

壹、概說

濫發電子郵件現象對整個網際網路之商業經營及經濟層面造成嚴重影響，甚至危及網際網路之正常使用與生態，對世界各主要先進國家所積極規劃的網路運用發展計劃形成嚴重之打擊。因此，越來越多的主權國家對這個問題作出積極的回應，制定法律加以規範。

從發生的時間先後順序觀察，全世界最早為美國內華達州於 1997 年訂立特別專法管制濫發電子郵件，隨著濫發電子郵件現象於 1998 年以後轉劇，美國又是世界上濫發電子郵件數量最為龐大的發出地區，各州相繼訂定管制濫發電子郵件專法。至本研究期間截止，已有三十六州完成立法。但是同一時期，歐盟針對資訊化社會開放應用通訊服務所產生隱私保護問題，循序漸進，陸續通過多個相關指令，責成各會員國於期限內訂立相關法律實施其規範，鋪陳出一個整體的保護個人隱私與消費者權益的法規架構，其成績令人矚目。在亞洲太平洋地區，日本、韓國作為寬頻網路建設之先進國，分別已在 2002 年在立法反制濫發電子郵件的序列中就定位。澳洲也積極不讓日韓專美於前，在 2003 年 11 月底通過以收件者事前同意為基礎的管制濫發電子郵件法案；而中國作為逐漸被指名為僅次於美國有數量龐大濫發電子郵件輸出的地區，產官學界也已形成共識，積極發起遊說政府進行相關管制濫發電子郵件立法工作。

美國於 2004 年 1 月 1 日起，將施行聯邦立法之 CAN-SPAM ACT，尤其成為舉世關注的焦點。無疑地，透過制定法律加以規範濫發電子郵件問題，已經形成了國際趨勢。我們可從下列四個面向觀察這個國際趨勢，並將在本章總結進一步分析，國際上對抗濫發電子郵件所須面對的難題與發展方向：

一、 歐盟的積極立法作為帶動全球規範濫發電子郵件之立法風潮

從歐盟 Directive 97/66/EC「電信部門下之個人資料處理及隱私權保護指令」、Directive 2000/31/EC「資訊社會各項應用服

務中內國市場電子商務之法律議題指令」到 Directive 2002/58/EC「電子通訊下個人資料處理及保護個人隱私指令」一路發展下來，我們看到，歐盟完整以隱私保護為軸心建構的網路秩序規範，透過其指令實施的強制，漸次統合歐洲各個經濟強權，在網際網路新紀元處理濫發電子郵件現象所帶來多項交錯複雜的權益衝突問題的共同立場，進而擴張其影響力到各個重要的國際組織，包括聯合國及經濟合作發展組織，呼籲世界其他國家採取與歐盟相同或貼近之立場，以縮短國際合作解決濫發電子郵件問題所可能耗費的冗長溝通時間，儘速建立有效遏止濫發電子郵件現象繼續擴大蔓延的執行機制。歐盟執委會對美國國會在討論 CAN-SPAM ACT 法案之際，積極遊說美國採取相同的事前同意機制，尤其顯示歐盟在本議題上擔任火車頭帶領國際立法風潮的決心。歐盟執委會負責企業與資訊化社會事務的委員 Erkki Liikanen 強調，各國政府必須趕在濫發電子郵件摧毀全球使用者對於網際網路及行動通信網路的信心之前，全面對濫發電子郵件者宣戰。其具體戰略則是各國應盡量依相同標準來管制濫發電子郵件，不使濫發電子郵件者有機可乘，鑽營各國管制法令漏洞，繼續對網際網路使用秩序造成威脅。

長遠看來，歐盟各國在廣大的歐洲市場以歐盟指令作為其國內規範濫發電子郵件之立法依循，極有可能影響其他研究制定管制濫發電子郵件法律的國家，仿效歐盟指令立法之結構與方式做為其參考之指標。

二、Opt-in 與 Opt-out 機制之取捨

美國 CAN-SPAM ACT 立法，在微軟公司領軍由直銷協會(Direct Marketing Association)出面積極遊說國會，就管制濫發電子郵件立法確定採取事後拒絕機制(Opt-out) ，在這個維護商業利益立場上進行遊說的利益團體並不掩飾，其憂懼重新再有起色的網路商業在對抗濫發電子郵件者的法律戰爭中，一併和不法的行銷業者陪葬，而積極動員國會議員朝其希望維持既有網路行銷模式，但消除網路匿名效應的設計提案。但是，美國 CAN-SPAM ACT 採取事後拒絕機制立法管制方式，對於亞洲的日本與韓國等前已確立採取事後拒絕機制反制網路上濫發電子郵件行為的國家，似乎是更提醒他們，在隱私保護之外以推動全球化網路商業為國家發展目標的政府，不宜輕言犧牲或因此延緩重商主

義實踐的腳步。

與此相對的是，歐盟立下典範的事前同意機制(Opt-in) ，管制所有商業及電子郵件發信人，在取得收件人事前明示同意之前不得發送商業性質之電子訊息。澳洲緊隨歐盟立法腳步，也採取相同原則完成立法。理論上，事前同意機制對於收件者個人隱私提供之保護程度應該遠高於事後拒絕機制。但是，實踐上，各個國家立法並未嚴格地或徹底地傾向採取事前同意機制或事後拒絕機制。採取事前同意機制立法的國家，包括英國及歐盟其他會員國，甚至澳洲都在所謂事前同意的定義上，開闢例外緩和正常商業活動可能受到的不便和阻礙，實際上變成一種妥協的事前同意機制，而採取事後拒絕機制立法的國家，例如美國及韓國，若不單以立法內容評斷，而一併檢視其執行做法及相關配套措施，包括民間 ISP 業者與消費者保護團體積極動員反制濫發電子郵件的活動情形，似乎結果上並不遜於事前同意機制實施的成效。時間終究會證明孰能擅場。

三、立法規範後仍須面對之難題

雖然立法管制濫發電子郵件問題已經成為國際趨勢，然而，以美國的情形來看，即使國內已經有超過三十州訂立州法管制濫發電子郵件，美國仍然是世界上濫發電子郵件之最大來源國，由此看來，光靠立法管制尚無法達到有效的控管目的，使濫發電子郵件問題從此消失。

在本所與雅虎國際公共政策總監 Dr. Stephen Collins、韓國國家安全局個人資料爭議委員會秘書長 Dr. Hyu-Bong Chung, Ph.D.，以及英國國會議員 Brian White MP 之訪談內容中受訪者皆曾提到，依賴立法規範濫發電子郵件並不能徹底阻絕此問題，即使訂立再完美、再嚴謹的法案，由於網際網路無遠弗屆的特性，在法案的執行上還是得面對濫發電子郵件者隱藏 IP 位址、造成追蹤困難以及選擇未制定專法國家規避法律追訴等等難題。因此，在立法規範濫發電子郵件問題之後，各國政府乃至於民間 ISP 業者仍須持續關注，並擬定長遠計劃共同對抗，才能收到遏止之效。而這些後續防制方法分別包括：科技改良、

教育普及、國際合作[37]、兼顧不同文化基礎調整作為(例如建立線上戳記系統鼓勵網路使用者共同參與監督)[38]。另外，如何面對因濫發電子郵件技術的進步與電腦病毒攻擊之結合，亦是在管制濫發電子郵件問題時所不可忽略，並需要結合法令與科技的共同努力加以對抗的重要議題[39]。

以上所述，並不意味立法本身對濫發電子郵件問題無法收到實效，僅僅具有宣示作用。即使實際執行管制濫發電子郵件法律的成效並不如預期，然而立法本身除了具有宣示正視濫發電子郵件問題的作用，亦提供了一套良好的商業規則，以供電子商務經營者及網路服務業者遵循，並讓市場參與者知道其底線，明白其權利基礎。由此可知，立法規範濫發電子郵件問題仍然有其功用及價值存在，其意義就如同訂立刑法並不等同社會上所有犯罪問題便會就此消失一樣[40]。

四、國際合作之必然性

在談論到管制濫發電子郵件法規之執行時，不可避免必定要面對發生在網際網路上法律糾紛其準據法的適用，以及管轄權究竟誰屬之問題。此乃因網際網路係一跨國性的空間，雖然非屬任何一個國家，但其非物理性、跨國界以及去中心化（decentralized）的特性似乎使得各國對網際網路上的行為皆有管轄權[41]，而且使準據法的決定產生困難。有關這一點，在美國以及澳洲管制濫發電子郵件的法律裡，都出現明文規定擴張其法律適用至域外之效力之情形

傳統的法律體系囿於國界的限制，具有嚴格的地域限制，一國的內國法律並不當然具有域外效力，因此當這種傳統法律效力遇上網際網路時，光靠內國法規範網路行為的不足之處便

[37] **請參考附件三**--- 訪問雅虎國際公共政策總監Dr. Stephen Collins有關管理濫發電子郵件問題之訪談紀錄 2003/10/01

[38] **請參考附件四**--- 訪問韓國國家資訊安全局個人資料爭議委員會秘書長 Hyu-Bong Chung, Ph.D.有關管理濫發電子郵件問題之訪談紀錄 2003/10/01

[39] **請參考附件五**--- 訪問英國國會議員Brian White, MP（Member of Parliament in the United Kingdom and Treasurer of the All Party Parliamentary Internet Group）有關管理濫發電子郵件問題之訪談紀錄 2003/11/06。

[40] **請參考附件三及四**--本所與雅虎國際公共政策總監及與韓國國家安全局個人資料爭議委員會秘書長之訪談紀錄。

[41] 宋皇志，＜WTO/TRIPS架構下專利侵權的新態樣：為販賣之邀約＞，月旦法學雜誌 99 期，頁 145。

立刻顯現出來。濫發電子郵件問題正是一個最佳例子，即使一國的內國法訂立嚴格的法律規範濫發電子郵件行為，濫發電子郵件者仍能遷移至其他未訂立相關法律規範的國家繼續濫發電子郵件，本研究訪談英國、澳洲、韓國及美國管制濫發電子郵件法律的執法者發現，其異口同聲強調，其執法工作重點在於，有效減少源自其內國濫發電子郵件的數量-所謂各人自掃門前雪，也掃他人瓦上霜，一定可以在短期內見到成效。因此，如何促進濫發電子郵件法規地域性的趨弱及國際性的加強，將是各國在訂立法規之後所必須嚴肅對待的課題。藉著國際合作，甚至透過訂立國際性或區域性公約，來統一各國管制濫發電子郵件法規的標準與做法，則是打破法律規範地域性限制的關鍵步驟。韓國及澳洲在亞洲太平洋地區，已經朝此願景跨出一步，由兩國隱私權保護主管機關簽署合作備忘錄，值得注意後續在本地區的擴大合作效應。

貳、美國

一、濫發電子郵件對網路使用造成的影響

美國微軟公司總裁比爾蓋茲(Bill Gates) ， 2003 年 11 月 17 日在美國 Comdex 年度大型電腦展覽會開幕演說中指出，濫發電子郵件已經成為全美國網路使用者申訴威脅網際網路使用安全排名第一的現象，比起排名第二的電腦病毒網路，使用者申訴的比例還超過三成。根據美國非營利組織 Pew Internet and American Life Project 在 2003 年 6 月抽樣調查全美國 1,400 名網路使用者結果發現，濫發電子廣告郵件在美國已經泛濫到擋也擋不了的程度。三分之二的受訪者都試過依所收到電子廣告郵件指示的方法表明取消訂閱，但是他們發現接下來收到的濫發電子廣告郵件反而有增無減。超過半數受訪者說，濫發電子廣告郵件實在太多，多到讓他們很難找出想要看的電子郵件。結果，大多數受訪者都表示，他們現在已不會在網站上提供電子郵件地址，以防收到更多濫發電子廣告郵件。也有許多受訪者說，他們無論在家或在公司，都已使用軟體程式過濾濫發電子廣告郵件。聯邦貿易委員會(FTC) 2003 年發布的一份相關調查報告則顯示，超過六成以上商業性的濫發電子郵件(UCE)內容涉嫌不實詐欺。

現實結果便是濫發電子廣告郵件已經使一半美國網路使用者對所有收到的電子郵件都不再信賴，四分之一的網路使用者因為濫發電子廣告郵件無法阻擋而已減少使用電子郵件[42]。美國雅虎總公司統計，該公司使用的過濾軟體可以成功阻擋全部濫發電子郵件的半數，其餘半數還是以各種掩飾方式滲透進了其網路使用者的信箱：這些濫發電子郵件將近有百分之八十五來自美國本土，另有百分之十五來自歐洲，以及一小部份來自亞洲。因此，美國許多大型ISP業者，例如American Online（AOL）以及CompuServe（CSRV）等，為了保障其用戶之權益以及妥善其伺服器系統之維護，紛紛向法院對這些濫發電子郵件者（spammer）提出控訴，要求法官頒發禁制令，禁止濫發電子郵件者繼續發送電子郵件騷擾他們的用戶。早前也有數個州立法，以反映網路使用者對於濫發電子郵件亟待政府出面管制的心聲，而在以聯邦立法方式阻止濫發電子郵件問題繼續擴大的進度上，美國總統布希在 2003 年 12 月 16 日簽署國會通過的「控制不請自來之色情暨行銷侵襲法」（Controlling the Assault of Non-Solicited Pornography and Marketing Act，簡稱為CAN-SPAM Act of 2003，「濫發電子郵件法」），足見濫發電子郵件問題在美國影響到人民生活，所受重視之趨勢。但是，也不可避免地引發限制濫發電子郵件是否合憲之爭議

二、美國管制濫發電子郵件合憲性之探討

（一）商業性言論自由與美國憲法第一條修正條文

關於濫發電子郵件是否應受到美國憲法言論自由的保障，從而不許ISP業者以訴訟方式請求排除或禁止，牽涉到商業性電子郵件是否為一種商業性言論的表達。因為直到 1976 年 America Virginia States Board of Pharmacy v. Virginia Citizens Consumer Council一案，美國聯邦最高法院才以判決確認了商業性言論應受到美國憲法第一條修正條文的保障，若非請自來之商業性電子郵件（UCE）屬於一種商業性言論的表達，即可援引前例受到憲法第一條修正條文之保障[43]。

[42] See http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=3670439, (visited on 2003/10/24)

[43] See Joshua A. Marcus, *Commercial speech on the internet：spam and the first amendment,* Cardozo Arts & Entertainment, Vol. 16:245, 1998, at 260-274.

美國聯邦最高法院在Central Hudson一案中，對商業性言論的定義是「純粹是與言論者及閱聽者經濟上利益有關的表達」[44]，我國學者對於此處所指商業性言論的定義則註解為，「凡是宣傳或推廣某種商品或服務的言論，而其目的在直接刺激該項物品或服務的交易，以獲取商業利益者，均是所謂的商業性言論」[45]。因此，若非請自來商業性電子郵件內所傳遞的訊息，是以宣傳、推廣商品或服務，並刺激其交易以獲取商業利益者，即是屬於商業性言論。

然而在一封傳遞商業性訊息的電子郵件中，也有可能另外參雜了其他有關政治性或宗教、文化之言論，且由於非商業性言論目前在美國實務上仍認為較商業性言論擁有更完全的憲法保障[46]，因此有可能會發生以商業性言論搭配非商業性言論，來獲取更強的言論自由保障的情形出現。在此種情形，學者認為仍須以其整體言論來推斷其主要目的是否在推銷其商品或服務，若是，則不應以其參雜其他非商業性言論，而認為應受到與非商業性言論同樣強度的保障。

（二）商業性言論的合憲性審查標準及原則

傳統上依據憲法第一條修正條文對言論自由保障所建立之審查基準有下列四項原則，即時間、地點或方法限制（time, place or manner restriction）原則。政府對於言論自由的限制符合下列四個要件即為合憲：

(1)不得以言論內容決定時間、地點或方法的管制（content neutral）；
(2)此管制已被調整；
(3)此管制能夠實質促進一項重要的國家利益；
(4)言論在此管制外仍有其他替代的通訊管道可以對外表達。

[44] *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S.（1980）at 561.
[45] 林子儀，＜商業性言論與言論自由＞，美國月刊，二卷八期，七十六年十二月，24 頁。
[46] 美國聯邦最高法院在*Virginia States Board of Pharmacy v. Virginia Citizens Consumer Council*（1976）一案中及*Ohralik v. Ohio State Bar Ass'n*（1978）一案中，雖然都肯定商業性言論應受到憲法第一修正案之保障，然亦均陳明其保障強度應較非商業言論來得低之見解，see Joshua A. Marcus, *Commercial speech on the internet：spam and the first amendment,* Cardozo Arts & Entertainment, Vol. 16:245, 1998, at 262-264.

在 1980 年的 Central Hudson Gas & Electric Corp. v. Public Service Commission of New York 一案中，聯邦最高法院更確立了以四階段審查基準來檢驗對商業言論的管制是否合憲。此四項審查基準為：

(1)該言論所涉及者必須是合法行為，且非引人錯誤的商業言論；
(2)政府對於訂頒法令限制商業言論，有實質利益；
(3)對該商業言論的限制係為直接促進前述之國家實質利益的實現；
(4)限制必須被限縮調整到能符合國家利益為限，亦即政府對商業言論的限制必須是最小限度，未逾越為促進國家實質利益的實現所必要的程度[47]。

依上述基準，所有目前由美國國會審議中反制濫發電子郵件的法案似乎皆應受到較寬鬆的檢驗才是。

另外，在決定網路商業性言論的憲法保障強度時，應先討論及網際網路的媒體屬性。網際網路究竟是否與傳統的廣電傳播媒體（包含廣播及無線電視）相類似？由於廣電媒體具有普及程度高及影響力深遠的特性，對於幼童及未成年人也有較容易接近的特點，因此實例上較少受到第一修正案的保護。也許廣電媒體是與網際網路最類似的媒體，這是否即意味者，網際網路也必須如同廣電媒體般受到較強的規制及較少的言論自由保護？然而在著名的Reno[48]案中，法院卻拒絕將網際網路類比為廣電媒體，因為法官認為網際網路上的通訊不會在未經要求下侵入個人住家或出現在個人電腦螢幕上。然而，此項判決見解，衡諸目前網際網路應用實況，顯然不適用在這裡所討論的濫發電子郵件問題上。

前述 Reno 案的判決結論，將網際網路認定為一個全新且獨特的世界性通訊媒體，並認為其獨特之處有以下四點：

(1)網際網路之進入障礙極低；
(2)這個進入障礙對言論發表者及接收者兩方來說是相同的；
(3)障礙極低使得網際網路上的內容多樣化；

[47] See Joshua A. Marcus, *Commercial speech on the internet：spam and the first amendment,* Cardozo Arts & Entertainment, Vol. 16:245, 1998, at 255-256.
[48] *ACLU v. Reno*, 929 F. Supp. At 842-844（1996）

(4)對於想在網際網路上發表言論的人，網際網路提供重要的管道，甚至對每個言論者創造了對等的地位。

Reno 案的法官認為網際網路應較其他的媒體受到更多憲法第一修正案的言論自由保護。原因在於，網際網路相對於傳統的廣電媒體而言是一個更民主的媒體，所以可以受到較寬廣的保障。但是對於非請自來商業性電子郵件，恐怕很難適用到這個理論來賦予其發信人所謂憲法保障的言論自由。因為，對於被強迫收閱這些非請自來濫發電子郵件的人而言，實在無從認同這種入侵個人電腦的現象是民主精神的體現。也因此，本研究所檢視美國學界多數對網路上擾人（intrusive）的廣告都主張不應賦予其發信人任何在憲法第一條修正條文下擴大的保護。

(三)管制濫發電子郵件法案合憲性之探討

由前述美國聯邦最高法院在 1980 年的 Central Hudson Gas & Electric Corp. v. Public Service Commission of New York 一案中所確立的四階段違憲審查基準，來檢視美國聯邦及各州管制濫發電子郵件法案合憲性，可以進一步分析如下：

1.商業性言論是否合法且非引人錯誤

由於非請自來的電子郵件，種類上除了其內容不法或有引人錯誤的電子郵件外，還可能包括了內容合法且無引人錯誤的廣告電子郵件，縱使這些郵件為非請自來，若其內容為合法且無引人錯誤，則仍像其他形式的商業言論一般，受到美國憲法第一修正案之保障。

2.政府對此規制有無實質利益

在目前管制濫發電子郵件的法案中，政府對這些管制行為有無實質利益，可由以下三個不同理由來討論：

（1）阻止費用不當轉嫁（cost-shifting）：

由於大量的濫發電子郵件傳輸會導致 ISP 業者的頻寬被佔用，導致 ISP 業者須花費大量的金錢來建置更多的頻寬。但

是這些建置頻寬的費用最後仍會轉嫁到收件者的身上，使得收件者必須付更多的金錢才能使用接收信件的服務。而收件者瀏覽或刪除濫發電子郵件，也需花費額外的時間及金錢，最後造成整體社會付出可觀的經濟成本。政府若能保護收件者或消費者免於此種經濟上的損失，自然可看成是一項實質的國家利益。

（2）避免個人的隱私權遭到侵犯（invasions of privacy）：

政府是否有保護人民隱私之實質利益，其爭議較大，此可由法院實務過去在 Rowan v. United States Post Office Department（1970）一案以及 Bolger v. Youngs Drug Products Corp.（1983）一案中之見解加以分析。在 Rowan 案中，法院認為政府有維持及保護人民居家隱私尊嚴的實質利益，但仍有學者評論認為，非請自來電子郵件廣告的收件者其實就與傳統上寄到家門前的垃圾郵件收件者處境相當，只要忍受多看一眼，或者只須移動滑鼠即可將不需要的訊息刪除掉。然而 1983 年的 Bolger 案判決做出後，美國多數法院判決例遵循且繼續主張隱私保護是有力的政府利益，因此保障個人隱私對政府具有實質上利益[49]。

（3）終止對 ISP 業者財產權的侵害（trespasses to property）：

對於財產權的保護能否成為政府規制商業言論的實質利益，應視該財產的公共性質及目的加以具體判斷。從濫發電子郵件發信人濫發電子郵件造成 ISP 業者網路系統過度負擔，影響網路使用者迅速取得網路資源及其他加值性服務之目的以觀，此財產權保護應可認為是管制商業言論的實質利益。

3.該管制是否直接促進國家利益的實現

聯邦最高法院判決例認為，其是否能促進國家利益的實現，須到達直接且重大的程度。禁止濫發電子郵件的法律，雖可阻止或減低廣告主藉由濫發廣告信件而將其費用轉嫁到收件者及 ISP 業者身上，但是，這樣的管制措施是否能「直接」促進國家利益的實現，似乎不無疑問。參引聯邦最高法院在

[49] See Kenneth C. Amaditz, *Canning "Spam" in Virginia：Model Legislation to Control Junk E-mail*, 4 Va. J.L. & Tech. 4（spring 1999）; http://vjolt.student.virginia.edu/graphics/vo14/home_art4.html (visited on 2003/09/26)

Destination Ventures v. Federal Communications Commission[50]一案中表達的見解，類似管制能直接促進國家利益實現的看法，應該可以獲得肯定。

另外，在 United States v. Edge Broadcasting Co.一案中，法院也支持政府的規制可採漸次解決方式，不需要一次完全消除費用轉嫁問題[51]。

4.此規制是否逾越促進國家實質利益的實現所必要之程度

在考量是否逾越促進國家實質利益實現的必要程度，首先應考慮兩個要件：

（1）應仔細計算言論發表的成本及相對人的負擔；
（2）有無其他較低成本的選擇。

立法限制大量濫發電子郵件應該可以避免大量的網路使用費用被不當轉嫁，而且似乎也沒有其他花費較少的選擇足以促進上述國家利益的實現，因此這樣的管制應無逾越促進國家實質利益實現所必要的程度。然而，管制濫發電子郵件的立法如果有下列情形，則有可能被認為逾越必要程度，例如：

（1）全面禁止大量發送商業性電子郵件：

由於此種立法要求發信人需個別取得收件者同意，實行上誠有困難，而且如此一來新商務關係的建立完全處在被動地位，與一般社會觀念認為業者應主動行銷的習慣有違，較有可能被質疑違反憲法第一修正案。

（2）過度增加 ISP 業者或網路使用者的負擔：

例如立法要求 ISP 業者安裝過濾軟體程式並不能避免 ISP 業者及網路使用者負擔因不當轉嫁所產生的支出，反而更加重其負擔，同樣會造成不當轉嫁的情況發生，只是與濫發電子郵件發信人的不當轉嫁行為呈現不同的面貌而已，可能也有違憲之嫌。

[50] *Destination Ventures v. Federal Communications Commission*, 46 F.3d 54（9th Cir. 1995）
[51] *United States v. Edge Broadcasting Co.*,509 U.S. 434（1993）

（3）安裝過濾軟體程式：

若立法要求以科技方式過濾封鎖信件，執行不當可能造成連同意收受濫發電子郵件的人也收不到其電子郵件；同時也可能將不是濫發的電子郵件擋除在收件者的信箱之外，造成執法上的重大瑕疵。

綜上所述，管制濫發電子郵件的法案會不會造成違憲問題，仍須視法案規範的具體內容來論定。但是在這些法案規定，ISP 業者可對濫發電子郵件發信人提出損害賠償訴訟，減少政府對網路上濫發電子郵件問題的干涉；或是由 ISP 業者建構一個使收件者可以拒絕發信人繼續發送郵件的機制（Opt-out），由收件者為其是否接收濫發電子郵件的最終決定者，則無違憲之顧慮[52]。

三、目前美國管制濫發電子郵件立法之發展現況

（一）現有美國聯邦立法規範

1.美國聯邦反濫發電子郵件立法之發展歷程

以往美國用來阻止大量濫發電子郵件之法律，並非係針對大量濫發電子郵件行為所設立之特別法。總括來說，該等法律包括電腦濫用法、智慧財產權法及不成文法中有關禁止不當擾亂行為（nuisance）及禁止侵入他人財產（trespass）之判決例。

美國眾議院商業委員會在 2001 年 3 月，即初審通過了一項反濫發電子郵件法案，該法案主要採取 Opt-out 機制，使收件者有權要求將自己的電子郵件地址從濫發電子郵件者的發送名單上去除，且濫發電子郵件者必須於郵件上提供一個有效的發信人電子郵件地址。未能按規定執行的業者將被處以 500 到 50,000 美元的罰款。

[52] 蔡淑美，＜網路廣告與消費者保護民事法律問題之研究＞，國立成功大學法律學研究所碩士論文，民國八十九年六月，167-176 頁。

在 2003 年 7 月，美國眾議院司法委員會下屬的犯罪、恐怖主義和國土安全委員會亦對一個名為「減少濫發電子郵件法案」（Reduce Spam Act）進行聽證。該法案的主要內容包括:任何人不得發送「商業性質的電子郵件」，除非接收者有權選擇退訂（Opt-out）；ISP 業者可以對濫發電子郵件的發信人向聯邦法院提起訴訟，要求罰款，如果法官認定被告的發信人是「故意」違法，那麼罰款金額將高達 150 萬美元。此外，發送任何包含與色情相關內容的電子郵件以及偽造發信人身份的行為也視為犯罪，最高可處兩年以下有期徒刑。如果 ISP 業者證明其利益因濫發電子郵件的發信人行為受損，可以請求依每封濫發電子郵件五百美元計算的損害賠償。

2003 年 10 月，美國參議院以 97 票對 0 票表決通過一項反濫發電子郵件法案，決定要限制濫發電子郵件，並將設立「拒絕收信」（do not spam）的登記制度，讓不想收到不請自來商業電子郵件(UCE)的民眾登記。但是，在收件者未提出停止寄發的要求之前，行銷業者可以繼續寄發電子郵件。

與上述眾議院聽證中「減少濫發電子郵件法案」不同的是，這份法案並未禁止發送所有未經收件者同意的商業電子郵件，反而比較著重在管制不實或詐騙的訊息，凡回郵電子郵件地址造假，在郵件主旨欄以類似「Re: your request」（回信：你的請求）等字眼來隱藏廣告訴求，或者是推銷強身藥及其他不實廣告產品者，皆可處一年以下有期徒刑，以及一百萬美元以下的罰金。累犯者可處五年以下有期徒刑。另外，濫發有色情內容的電子郵件，發信人必需加註明確的「性」訊息讓收件者可以過濾。這項法案也禁止寄發未經收件者同意的訊息給「拒絕廣告」名單內的消費者，這與稍早之前聯邦貿易委員會（FTC）開始實施的「謝絕來電」（Do not call）反電話行銷做法類似。

其他濫發電子郵件者的常用技倆，諸如在網站上蒐集網路使用者的個人資料，利用多個電子郵件地址逃避過濾功能，用隨機亂數法則產生數百萬個電子郵件地址大量寄發郵件等等，也都屬非法行為。州與聯邦執法者及 ISP 業者，將可對濫發電子郵件者起訴，但個人使用者則不能直接為原告起訴。

行政機關方面，布希政府表示支持這份法案[53]。因此，隨後聯邦的反濫發電子郵件立法就循此法案，加速審議的腳步，而誕生了第一部相關的法律。

2.美國聯邦新近通過之濫發電子郵件法(CAN-SPAM ACT of 2003)

在 2003 年 11 月 22 日，美國眾議院表決以 392 票對 5 票懸殊的比例通過「控制不請自來之色情暨行銷侵襲法」（Controlling the Assault of Non-Solicited Pornography and Marketing Act），簡稱為「濫發電子郵件法」(CAN-SPAM ACT)[54]，同年 11 月 25 日經美國參議院修正通過。美國總統布希於同年 12 月 16 日簽署，成為美國聯邦第一項管制濫發電子郵件的法律，預定在 2004 年 1 月 1 日正式施行。

儘管這個法案在國會得到空前的支持通過，各方評價卻是出現兩極走向。支持本項立法的 ISP 業者認為，反濫發電子郵件立法目的，本來就不在於管制濫發電子郵件，而是規範直銷作為。因此，對於美國其他尚未就反濫發電子郵件有相關立法的州而言，本法適時通過有規範填補的作用，並為跨州交易性質的電子商務樹立了一致可遵循的商業行為準則。但是，大部分倡言嚴格限制濫發電子郵件的專家學者仍對這項法案的內容及其實施的效果感到悲觀，因為這項法律等於正式將濫發電子郵件行為合法化，並可能導致濫發電子郵件之數量繼續增加。就如大部分仍在國會參眾兩院待審的其他反濫發電子郵件法案一樣，這個法律一開頭說明其宗旨時也指稱：「由於電子郵件的方便性及效率性之特徵，以電子郵件發送未請自來的行銷訊息者越來越多……而這個數字正不斷地急速擴張中。」批評這個法律將濫發電子郵件行為合法化的立論基礎，在於這個法律乃是採取所謂的 Opt-out 機制，也就是其允許任何人皆可濫發未經收件者許可的電子郵件訊息，只要其發送訊息中有包含可讓收信者拒絕往後繼續接收郵件的機會即可。相反的，Opt-in 機制則是除非發信人事先因基於先前與收件人間契約或類似商業關係而得知收件者之郵件地址，或已事先得到收件者之同意，否則一律禁止發信人寄送任何未經許可的電子郵件訊息。假使如本法開宗明

[53] See http://news.com.com/2100-1028_3-5095408.html?tag=prntfr （visited on 2003/10/29）

[54] **請參考附件六---**美國聯邦有關管理濫發電子郵件相關法案“ Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003” or the “CAN-SPAM Act of 2003”

義所示，減少濫發電子郵件之數量是反濫發電子郵件法案之重要目的之一，那麼採取 Opt-out 機制之法案似乎很難達成這個目標。

儘管，濫發電子郵件之數量似乎是管制濫發電子郵件問題之惟一癥結所在。CAN-SPAM ACT 亦透露其對濫發電子郵件內容擔憂之一面，因為在這些濫發電子郵件中，通常也包含了許多充滿詐欺及色情之犯罪行為，而 CAN-SPAM ACT 對這方面有許多相關規定：禁止濫發電子郵件之主旨或內容裡包含錯誤或誤導他人之訊息，並要求這些濫發電子郵件須清楚地表明其廣告性質；除非郵件標示聯邦貿易委員會將來所設計的識別標籤，否則禁止任何有關色情之內容在郵件的開頭或連結的網頁中顯示出來（即使在郵件的首頁或開頭只是包含連往色情網站之連結，也在禁止之列）。

即使有這麼多的條文對濫發電子郵件行為做相當之管束，很多支持嚴格管制濫發電子郵件現象的評論仍然認為 CAN-SPAM ACT 效力太過薄弱，且可能遭到比較強勢的州法所取代。美國全國檢察長協會底下之網際網路委員會（the Internet Committee of the National Association of Attorneys Gereral，State AGs）曾經於 2003 年 11 月 4 日就審議中的 CAN-SPAM ACT 法案發函美國眾議院表示，他們認為 CAN-SPAM ACT 法案開啟了許多漏洞及後門，以及設下高規格的舉證責任規定，使得極少數的消費者得透過此法案得到保護，而主管機關及檢察官在執行法律時卻須負擔太多責任等等。而在此法案已經經過許多修正並完成立法以後，該委員會仍然不改其批評之態度。

以下針對 CAN-SPAM ACT 中之重要規定詳細介紹：

（1）對於濫發電子郵件之定義

本法第三條中將濫發電子郵件定義為：「以商業廣告、商品或服務之行銷為首要目的而寄送之電子郵件訊息……」並排除先前已有交易或其他關係（Transactional or Relationship）之電子郵件訊息。所謂先前已有交易或其他關係之情形為：該封電子郵件之主要目的（Primary purpose）

為：

A. 收件者預先同意寄件人發送有關促進、完成或確認交易之訊息；

B. 對於收件人所購買之商品或服務發送有關提供擔保、商品回收或使用安全之相關資訊；

C. 寄送有關定期計算之收支，訂戶、會員資格、帳戶、借款或其他類似之現存關係之契約條文修改、收件者資格改變之提醒信函；

D. 提供直接與收件者有關之僱佣關係或相關之有利計劃之訊息；

E. 寄送收件者已基於契約內容而事先同意發信人寄送之有關商品或服務，包括產品升級之消息。

本法更進一步規定聯邦貿易委員會（FTC）應制定如何定義信件中之「主要目的」(Primary purpose)之相關標準，並賦予其得因應履行該法案目的之需要而調整濫發電子郵件定義之權力。然而，即使如此，在上述美國全國檢察長協會致眾議院之信件中，仍批評此法對於濫發電子郵件之定義開啟了一大漏洞，讓濫發電子郵件者可爭論其所濫發之電子郵件中之主要目的已超脫純粹廣告之範圍。

（2）關於「受到保護之電腦」之定義

在 CAN-SPAM ACT 中大部分有關規範濫發電子郵件定義為「來自」或「發送」至在電腦詐欺及濫用法案(Computer fraud and Abuse Act）中所定義之「受到保護之電腦」（Protected computer)。然而因受到美國於 2001 年立法的「愛國法」(Patriot Act)對美國司法管轄權空前膨脹至美國國界以外之影響，對於何謂「受到保護之電腦」也引起了些許爭議。根據其規定，所謂受到保護之電腦包括任何「用在跨州或跨國之交易行為，或即使該電腦位在國外，然而其主要之目的卻用於美國國內之跨州或跨國交易行為」之電腦。由於大多數之網路流量(Traffic)皆會通過美國境內，實際上地球上的所有電腦都可被該法涵括為其所謂「受到保護之電腦」。如此一來，適用 CAN-SPAM ACT 規範之電腦，即有可能包含地表上任何一台進行濫發電子郵件行為之電腦。

（3）與濫發電子郵件有關之詐欺問題

CAN-SPAM ACT 第四條禁止任何人從事下列各項行為：

A. 故意未經授權而入侵受到保護之電腦，並藉此散發大量未經同意之商業電子郵件；

B. 利用受到保護之電腦進行轉寄或傳送未經同意之商業電子郵件，並蓄意誤導收件人對信件來源之認定；

C. 大量寄送偽造主旨資訊之未經同意商業電子郵件；

D. 以錯誤資料申請或使用五個以上電子郵件地址，或兩個以上網路名稱，並蓄意經由上述電子郵件地址或網路名稱其中之一進行濫發電子郵件行為；

E. 以虛偽身分申請五個以上網際網路協定位址（IP address），並蓄意藉此濫發電子郵件。

所謂「大量」寄發意指在二十四小時內寄送超過一百封郵件，三十天內寄送超過一千封，或一年內寄送超過一萬封之郵件。違反上述規定，可處刑罰五年以下有期徒刑，並沒收其利用來作為濫發電子郵件之設備或工具。若被告先前已有犯下類似罪行，或那些濫發電子郵件寄送之電子郵件地址為經由未經許可之網站收集而來，或利用電腦以隨機亂數法則產生之電子郵件地址，則被告將被處以重罪罪刑(Felony)。

（4）在郵件內標示虛偽或使人誤導之資訊

CAN-SPAM ACT 第五條（a）款規定，禁止任何人寄送至受到保護之電腦未經許可之商業電子郵件，或基於先前已有交易或其他關係而寄送之郵件，而在其郵件內標示會使人陷於錯誤或誤導收件人之資訊。所謂在郵件內標示錯誤或使人誤導之資訊，包括一封郵件之來源、目的或路徑會使人陷於錯誤或使人受到誤導。

（5）郵件主旨為虛偽或使人受到誤導

CAN-SPAM ACT 第五條同樣禁止發信人在明知或可得而知該信件之主旨會使收件者對於該信件之內容錯誤認知之情形下，寄送未經許可之商業電子郵件（此條只有規範未經許可之商業電子郵件，並未包含基於先前已有交易或其他關係而寄送之電子郵件）至受到保護之電腦。

美國全國檢察長協會底下之網際網路委員會對此條文提出批評，認為：消費者保護法只要求有欺騙收件者的意圖或傾向便可能構成違法，然而此法卻要求須實際上將其欺騙的意圖顯現出來，才會構成違法，會使執法者面臨適用法律上的矛盾。

（6）Opt-out 機制

CAN-SPAM ACT 第五條規範 Opt-out 機制。這個條文禁止任何人寄送未經許可，且未包含有效回信地址使收件者可清楚且明白藉由回信表示其不欲繼續接收郵件機制之商業電子郵件。發信人可提供讓收件者得以選擇不繼續接收電子郵件之選單，以符合此條款之規定。

Opt-out 機制可容許收件者在收到不請自來的商業電子郵件後三十天內寄出其不欲繼續接受類似郵件的通知，發信人有無法控制之技術上問題時，則可容許收件者在問題修復後的合理時間內寄出其通知。如果收件者選擇不欲再接收郵件，發信人在收件者寄出通知後十個工作天後即不能再寄信給相同的收件者，發信人亦不得將收件者電子郵件地址出售、出租或轉提供給其他人。

美國全國檢察長協會認為 Opt-out 機制在條文設計上有許多問題存在。首先，他們認為製造 Opt-out 選單反而可能造成收件者的混淆，應該給收件者單一選擇不欲再繼續接收信件即已足夠，也就是完全的 Opt-out 機制（Total Opt-out）。其次，該協會亦反對法條中賦予發信人得因技術上問題而豁免之權利。該協會指出，這個規定可能造成規範上的大漏洞，因為濫發電子郵件者永遠可以辯稱，因為其技術上無法控制之問題而沒有辦法接到收件者所寄出的通知，因此，收件者的信箱內將

始終充滿濫發的電子郵件。該協會雖然承認應給予濫發電子郵件者相當時間，在收到通知後將該收件者自名單上刪除，然而十個工作天的時間也未免太長了些。

（7）信件上之廣告標籤

在本法第五條（a）款中規定，禁止任何人寄送未帶有明顯且清楚之廣告標籤之不請自來商業電子郵件至受到保護的電腦裡，但是，本法亦在第十三條中規定該廣告標籤並不限於任何形式。在本法施行後十八個月內，美國聯邦貿易委員會應對此廣告標籤之形式提出相關建議報告(例如於信件主旨上加上 ADV 或其他類似字樣之標籤)。

（8）發信人現實有效的郵遞地址(Postal address)

本法第五條（a）款中亦規定濫發電子郵件發信人必須在其發送的電子郵件中註明其現實有效的郵遞地址。

（9）電子郵件地址蒐集(Address harvesting)及字典式攻擊(Dictionary attacks)

本法第五條（b）款規定，任何從明示其網站使用者之電子郵件地址不可轉售或以其他方式洩漏的網站上蒐集電子郵件地址；或以自動排列字母或數字組合而產生之電子郵件地址而濫發電子郵件者，將會被以重罪處罰。

美國全國檢察長協會批評此條文並沒有禁止電子郵件地址蒐集或字典式攻擊的行為，而只有將這些濫發電子郵件者加重其刑而已。其認為應將上述行為獨立出來而予以規定禁止。而且，法條規定只有在明示其網站使用者之電子郵件地址不可轉售或以其他方式洩漏的網站上蒐集電子郵件地址的行為才受加重處罰，反而限縮了應該保護的個人資料範圍。

(10)色情郵件之警告標示

本法第五條（d）款中規定，除非收件者已有預先之同意，任何人不得於下列情況寄送含有色情資訊之不請自來商業性電子郵件至受到保護的電腦中：

A. 未在郵件主旨上標示聯邦貿易委員會在本法實施後120天內所核定之色情廣告標籤；

B. 沒有在郵件內標示上述之廣告標籤、Opt-out選單及有效的發信人郵遞地址；

C. 在郵件首頁便顯現這些色情資訊，使收件者一開啟郵件便可看到（相反的，應將這些色情資訊以超連結或其他方式在郵件中顯現）

所謂含有色情資訊之郵件指，郵件中包含任何直接涉及色情敘述或內容者，除非這些敘述或內容在整封郵件內只佔極小之部分，且郵件其它部分並不包含任何與色情有關之資訊。

(11)利用虛偽或使人受到誤導之主旨進行商業行銷之郵件

本法第六條規定，即使收件人明知或可得而知行銷行為的存在；或願意或期待收到有關該行銷行為之經濟上利益；甚或沒有採取任何阻擋收信或將該行銷行為報告給聯邦貿易委員會的動作，仍禁止發信人藉由標示虛偽或使人受到誤導之主旨發送郵件來進行任何有關商業、商品或服務之行銷行為。但除非該行為人擁有這個進行行銷行為企業之股份50%以上，或明知該行銷為利用虛偽或使人誤信主旨之不請自來商業性電子郵件所為者，否則無須對該次行銷行為負責。

依本法規定，美國聯邦貿易委員會專有執行此條文之權力。

美國全國檢察長協會對此條文提出兩點批評：第一，其認為沒有要求行為人需有 50%股份才需對其控制之企業行為負責之道理，否則大部分的行為人皆可輕易擺脫此條文之限制。第二，其認為聯邦貿易委員會沒有理由對此條文之執行專有執行之權力。

(12)聯邦貿易委員會及其他機構

本法第七條授權給聯邦貿易委員會執行此法案之權力。此外，遇有違反法案內若干有關經濟事項之規定時，包括聯邦存款保險公司（Federal Deposit Insurance）、證券交易委員會（Securities and Exchange Commission）、美國信用合作社管理局（National Credit Union Administration）及州立保險機構皆可對違法行為人提出告訴。聯邦貿易委員會可依其通常使用之合理方法來執行此法案，聯邦貿易委員會或聯邦通訊委員會（Federal Communications Commission，FCC）欲申請禁制令或下令行為人停止其行為時，亦無需舉證證明行為人明知其行為為違法（prove the state of mind）。

(13)美國各州之執行權力

本法第七條授權給州檢察長或其他適當之機關，在遇到其州內居民之利益遭受威脅或受到攻擊之情形，可對任何違反本法第五條規定之州內居民提起民事訴訟。州政府得請求其賠償實際上所受之損害或以每封濫發電子郵件二百五十美元計算，最高額為兩百萬美元之損害賠償，或申請禁制令。

然而州政府在聯邦已對該違反法律之行為展開行動，或在聯邦貿易委員會介入後，即不能再對之提起訴訟。審判地點可以在任何依據美國法典 28 USC 1391 規定之巡迴法院內進行，或由被告之住居所或營業所在地之管轄法院管轄。

(14)ISP 業者得採取之行動

本法第七條授與所有 ISP 業者得對違反法案規定之行為人請求發給禁制令或請求損害賠償，但並非針對所有的違法行為都可提起請求損害賠償。ISP 業者只能就違反第五條（a）第一款之郵件含有虛偽內容，及第五條（d）之未標示色情標籤，且僅只單次寄發郵件的行為提起訴訟；但對於第五條（a）第二款的標示虛偽主旨、第五條（a）第三款之郵件沒有包含 Opt-out 選單、第五條（a）第四款之未尊重收件者 Opt-out 之

選擇，及第五條（a）第五款之未標示廣告標籤及未包含發信人郵遞地址情況，除非該行為人一再地連續寄發這些郵件，否則 ISP 業者並無法對其提起訴訟。

令人不解的是，美國全國檢察長協會對這些看似過度限制 ISP 業者救濟權限，以及區別連續與單一寄發郵件之規定並未提出批判。ISP 業者對於上述可提起訴訟之情況，可對行為人申請禁制令，或請求下列之損害賠償：

A. 藉由 ISP 之服務發送或意圖發送違反第五條（a）第一款之郵件時，得請求每封郵件最高以一百元美金計算之賠償；
B. 藉由 ISP 之服務發送或意圖發送違反第五條其它規定之郵件時，得請求以每封郵件最高以二十五元美金計算之賠償；
C. 除了違反第五條（a）第一款之情形外，ISP 業者就行為人違反第五條規定最高可請求一百萬元美金之損害賠償。

(15)懲罰性賠償(Aggravated damages)

在州政府或由 ISP 業者提起訴訟的案件中，若被告為明知且故意違反規定，或涉及第五條（b）中所規定的蒐集電子郵件地址或字典式攻擊之情況時，法院最高可以判令被告給付三倍的損害賠償金額。若被告已盡相當之注意，且已建立及實施有效預防違反規定之方法或程序，或即使已盡合理之努力，仍無法防止違反法規行為發生時，法院得減少被告損害賠償之數額。

(16)律師費及訴訟費用

由州政府所提起之訴訟一旦勝訴，法院得判決被告支付合理之律師費及訴訟費用給州政府。而在由 ISP 業者所提起之訴訟方面，法院得要求 ISP 業者預為承諾支付所有訴訟費用，並於嗣後判決兩造負擔合理之訴訟費用及律師費。

(17)CAN-SPAM 與州立反濫發電子郵件法的適用關係

本法第八條直接賦予 CAN-SPAM ACT 在處理濫發電子郵件問題上取代所有州法的根據，除了州法規定濫發電子郵件中詐欺或虛偽不實資訊在郵件中所佔比例之規定外，其餘規定皆須依 CAN-SPAM ACT 之規範。由於美國許多州立反濫發電子郵件法之規定皆較 CAN-SPAM ACT 之規定來得嚴格（例如加州及德拉瓦州皆採 Opt-in 機制），美國全國檢察長協會指出 CAN-SPAM ACT 等於否定這些州管制濫發電子郵件問題之計劃，並在這些州以一套較弱之機制取代來規範濫發電子郵件問題。

然而，在下列情況，CAN-SPAM ACT 並不當然取代相關州法及 ISP 業者自定規章：

-該州之反濫發電子郵件法並不全然是針對濫發電子郵件予以規範，而亦包含以非法侵入他人動產、契約或侵權行為等規定來管制濫發電子郵件問題；

-州法中管制的濫發電子郵件問題另外牽涉到詐欺或電腦犯罪行為時；

-ISP 業者另外制定有關電子郵件之傳送路徑、轉寄、處理或儲存郵件訊息之規章時。

（18）「拒絕收信」登記制度（Do-Not-E-Mail Registry）

本法第九條要求聯邦貿易委員會應在此法施行後六個月內提出有關建立全國性「拒絕收信」登記計劃之報告及時程表，並在報告中將這個計劃所需之技術、安全性、隱私權保護及執行可行性一併考慮在內。然而，此法並不要求這個「拒絕收信」的計劃一定要被實行，其只要求聯邦貿易委員會可在此法施行九個月後開始進行此計畫。目前已有許多人，甚至包括聯邦貿易委員會主席 Timothy Muris 在內，對於這個計劃之可行性提出疑問。

（19）聯邦貿易委員會接下來需提出之報告

A. 本法第十條要求聯邦貿易委員會需在法案施行後兩年

內向國會提出有關本法之執行狀況及其影響，或法條有任何修正需要之報告。

B. 本法第十一條要求聯邦貿易委員會需在本法開始施行後九個月內向國會提出報告，介紹有關獎勵那些提供如何起訴違反法規者相關資訊之制度(Bounty system)。該制度之內容為：(1)此獎勵需頒發給第一個指認違反法規者，並提供如何向其請求民事賠償之相關資訊之人；(2)獎勵金額不得少於所有民事賠償額之 20%。然而，本法並無要求必須確切執行這個制度。

C. 本法第十一條亦規定，聯邦貿易委員會須於本法施行後十八個月內向國會提出如何在濫發電子郵件之主旨上標示其廣告性質之方法(例如於主旨上標示 ADV 或其他類似之字樣)。

（20）CAN-SPAM ACT 對無線傳輸通訊之其它規定

本法第十四條規定，此法中之所有規定並不影響既存聯邦法規中對於禁止傳輸不請自來商業廣告傳真或自動撥打電話系統之行銷電話之效力。另外，本法並要求聯邦通訊委員會（Federal Communications Commission，FCC）應於本法施行後 270 天內公佈保護消費者免於受到不請自來商業廣告傳真或自動撥打電話系統之行銷電話騷擾之規則，並在該規則中規定：(1) 除非消費者已預先對特定業者表示其同意接收訊息，消費者得選擇拒絕受到所有無線通訊傳輸訊息之騷擾；(2) 利用無線傳輸通訊系統進行行銷行為之業者，需在其系統中加入 Opt-out 機制，使消費者得表明其不想受到騷擾之意願。

（21）小結

濫發電子郵件行為的確對社會或個人、企業及經濟都產生許多問題，這些問題包括了騷擾、詐欺、影響頻寬和網路空間、郵件伺服器的負荷、影響正常電子郵件之收發、生產力下降、設備及人事增加支出、客戶抱怨及對網路使用環境之不信任，以及可能造成電腦病毒蔓延，都是使濫發電子郵件遭人厭惡之原因。這些原因可總歸成兩大部分：對於濫發電子郵件數量上及內容上之抱怨。大部分濫發電子郵件所引起的問題都是因為

其數量龐大所引起的，而對於抑制濫發電子郵件數量最好的方法，絕大部分的人都會同意採取 Opt-in 機制會比採 Opt-out 機制來得有效。這也是歐盟指令以及歐盟大多數會員國都採取 Opt-in 機制的原因。然而，CAN-SPAM ACT 採取的 Opt-out 機制，無異表示，除非收件者明白拒絕接收，濫發電子郵件者將可無限制發送郵件。這是 CAN-SPAM ACT 最大的問題癥結所在。

此外，此法還存在著許多缺點與不足之處，這缺陷在一開始對於濫發電子郵件之定義便已出現。此法對於濫發電子郵件之定義，乃是基於該郵件之「主要目的」是否涉及商業廣告或色情而決定。然而，濫發電子郵件者當然會辯稱其郵件之主要目的並非涉及商業或色情。其它的漏洞還包括，在郵件主旨或標題中標示虛偽或使人受到誤導之內容者，需主觀上具有故意才會造成違法，事實上濫發電子郵件者主觀上當然具有違法之故意，才會標示這些使人受到誤導或虛偽的標題作為主旨。而本法採取 Opt-out 機制之立法理由竟是認為 Opt-in 機制在技術上並不可行。無怪乎美國全國檢察長協會評論這部法律「引發訴訟爭議的功能遠比阻止不法行為之功能為大」。

看似可行的「拒絕收信」（Do-Not-E-Mail）登記制度在此法中並不強制需確切執行，在大部分主張嚴格管制濫發電子郵件的專家看來，這個登記制度則是不僅在技術上不可行，一旦完成，反而可能遭濫發電子郵件者利用來濫發電子郵件。至於，獎勵提供成功起訴濫發電子郵件者相關資訊之人的制度雖然普遍被認為可行，然而本法同樣亦不強制此項制度實施。

最後，本法還隱藏了另一個大缺失，其並無提供遭受濫發電子郵件騷擾之個人提起訴訟之權利，只有 ISP 業者、州政府及聯邦政府機關有為原告之資格得以提起訴訟。CAN-SPAM ACT 將自 2004 年 1 月 1 日起取代許多規範效力遠較為強的州立反濫發電子郵件法律，如果 CAN-SPAM ACT 是採取嚴格的 opt-in 機制，也許可以藉此整合雜亂無章的各州相關法規，訂立統一且嚴格的規範濫發電子郵件標準，然而事實上卻是相反。因此，許多投身反濫發電子郵件行動的專家擔憂，CAN-SPAM ACT 不僅將濫發電子郵件行為予以合法化，其數量上之問題還可能不增反減，讓危害更加擴大。這個爭議也只能等待時間來證明其結果了。

在已經完成立法的 CAN-SPAM ACT 之外，還有許多規範濫發電子郵件的法案在國會參眾兩院等待審議中，陸續將會出爐，包括：

-2003 年反濫發電子郵件法案（Anti-Spam Act of 2003）；
-禁止寄送詐欺性質之濫發電子郵件法案（Ban on Deceptive unsolicited Bulk E-Mail Act ）；
-電腦所有者權利法案（Computer Owners' Bill of Rights）；
-刑事反濫發電子郵件法案（Criminal Spam Act）；
-減少濫發電子郵件法案（Reduce Spam Act）；
-降低濫發電子郵件散佈法案（Reduction in distribution of Spam Act）；
-遏止色情及行銷行為濫用法案（Stop Pornography and Abusive Marketing Act）；
-防制透過行動電話系統無線電話濫發電子郵件法案（wireless Telephone Spam Protection Act）。

關於這些法案的相關內容，請參考【表 3.2 美國聯邦國會審查中法案之比較】。

3. 美國其他有關管制濫發電子郵件之法規

除了以上介紹管制濫發電子郵件之特別法，實例上，美國還有其他法規也適用於對濫發電子郵件行為的管制，茲分項說明如下：

（1）電腦詐欺及濫用法（Computer Fraud and Abuse Act）

本法於 1984 年訂立，立法目的係為保護聯邦政府中之資訊及聯邦政府電腦中所儲存之財務及信用資訊。但是，本法中所謂保護「電腦中之資訊」一詞，已被廣泛解釋為任何使用於「州與州之間或是與國外間之商業交易」之電腦[55]。在本法第十八章 18 USC 1030(a)(2)(c)中，規定「在州與州之間或是與國外間之商業交易，於未獲授權的情況下或是超過授權的範圍，故意取得或是讀取受保護電腦內之資訊，係為不合法之行為。」實例上，法院認為未獲授權取得他人之電子郵件地址係違反前述本法規定，而未獲授權取得

[55] See *Shurgard Storage Centers v. Safeguard Self Storage* (WD Wa. 2000).

他人之電子郵件地址，正是濫發電子郵件者之最主要行為[56]。

除此之外，該法第十八章 USC 1030(a)(5)(c)規定，禁止「任何故意讀取受保護電腦內之資訊，而造成超過五千美元損失之行為。」，實例上，法院認為散發數千封之電子郵件已違反這個章節之規定，因為該行為會破壞 ISP 業者之電腦網路及商譽。

（2）虛偽標示郵件來源（False Destination of Origin）

虛偽標示電子郵件來源可能違反藍哈姆法（Lanham Act，即美國聯邦商標法）第十五章 1125(a)(1)之規定。依照該規定，禁止任何人在商務上使用任何字、辭、姓名、象徵、圖案或組合或任何錯誤的起源頭銜、錯誤或引人誤信的事實說明、或錯誤或引人誤信的事實陳述、或可能對此人和其他人的關係、關聯或組合造成混淆、錯誤或欺騙；或對其他人所提供的商品或服務或商業活動的來源、贊助者或同意引起混淆、錯誤。由於濫發電子郵件者通常使用錯誤的電子郵件回覆地址，及欺騙收件者的標題來掩飾其濫發電子郵件的真正來源，而造成消費者混淆，因此，原告只須證明:

A. 被告使用標示；
B. 其行為是州際間之商業活動；
C. 該行為與商品或服務有關；
D. 其所標示之內容會導致他人對於商品或服務之來源、贊助者、或該服務或商品是否得到第三人之授權產生混淆；
E. 原告可能會因這樣的行為而遭受損害。

法院認為於電子郵件中之標題使用錯誤資訊標示，亦可構成對於第三人行使錯誤之表示或是文書[57]，即可適用藍哈姆法之規定。

美國聯邦法院即曾基於濫發電子郵件者的行為構成 15U.S.C. §1125(a)錯誤來源指示，及 15U.S.C. §1125(c)商標稀釋，而准許核發暫時性禁制令。

另外，在最近的美國法院訴訟中，以下兩個案件的原告也均援用藍哈姆法（Lanham Act）作為對抗濫發電子郵件者的主張：

[56] *AOL v. LCGM*, supra;
[57] See *America Online, Inc. v. IMS* (ED Va. 1998); *Hotmail v. Van$Money Pie 47 USPQ2d 1020* (ND Cal 1998); *America Online, Inc. v. LCGM, Inc.* (ED Va. 1998);

A. United Parcel Service of America Inc v. John Does One Through Ten（Case 103CV1639）

該案原告 United Parcel Service of America Inc（以下簡稱為 UPS）接獲數百名消費者的抱怨，稱其不停收到由 UPS 寄發的大量非請自來電子郵件，UPS 循線追查，最後對十名在幕後盜用 ups.com 作為其濫發電子郵件來源的人提起訴訟。這十名濫發電子郵件之人所經營之網站，是一家專門在賣成人用品的網路商店，其所經營的商業與 UPS 完全沒有任何關係。UPS 在起訴時，認為被告使用 ups.com 作為其信件來源，其主要目的有：

a.規避濫發電子郵件過濾軟體程式的過濾；
b.引誘消費者閱讀郵件；
c.避免其他濫發電子郵件者經常會遇到的管理障礙。

UPS 透過訴訟途徑，請法院核發禁制令，並判給損害賠償和律師費用。

B. Disney Enterprises Inc v. Prime Internet Network Inc（case 03-4901）

原告 Disney Enterprises Inc（以下簡稱 Disney）依照藍哈姆法（Lanham Act）之商標侵害（trademark infringement）、稀釋商標（trademark dilution）以及不公平競爭等訴因對被告起訴。該案被告在其大量濫發的電子郵件上違法使用 Disney 的商標，並偽稱消費者若將其個人資料回傳給發信人，就有機會至迪士尼樂園一遊，且附有連結至可讓消費者填寫其個人資料的網站上，致使收到信件的消費者上該網站將自己的個人資料透露給被告。原告主張該網站以 Disney 的商標為號召，更加深消費者認知上的混淆，誤以為 Disney 與這個網站有關聯，從而受到鼓動而在該網站上揭露其個人資料。Disney 起訴請求法院核發禁制令，並請求損害賠償和律師費用。

（3）稀釋商標之行為（Dilution）

州法或是聯邦法之規定都有規範稀釋商標權之行為。在聯邦法之下， 稀釋商標之行為係規範於 *Lanham Act* 第十五章 1125(c)(1)之下。該法規定，著名商標的所有人，不管其商標有無註冊，即可依 15U.S.C.§1125(c)主張反稀釋保護。

至於何謂商標稀釋，依該法的定義是，不管在著名商標所有人和其他人間是否存在競爭，或是否存在混淆、錯誤或欺騙的可能性，只要可能減低一個著名商標作為辨識及區別商品或服務的能力，即構成商標稀釋。因此，當原告主張被告行為使其商標作為表彰商品或服務的功能降低時，可以要求法院核發禁制令以阻止被告進一步的稀釋行為，如果被告故意導致對著名商標的稀釋，原告也可以要求金錢上的賠償救濟。

聯邦最高法院於 *Moseley v. Victoria Secret Catalogue Inc.*, 537 U.S. (2003)[58]案件判決出爐前，一貫認為當主張他方有稀釋商標之行為時，原告只須證明：

-原告對於該商標具有所有權；
-被告之標示將稀釋原告之商標權。

稀釋商標之行為包括為不利於他人商標之使用（tarnishment）。例如，被告將商標行使於形象不好的商品，或是被告商標會使原告商標特性不再顯著或是失去其表彰出處之功能。聯邦最高法院在 *Moseley v. Victoria Secret Catalogue Inc*. 一案判決改變其一向之見解，認為如僅證明原告對於該商標具有所有權以及使用被告之標示將稀釋原告之商標權，並不足以證明被告有稀釋商標之行為，原告必須證實其商標確有被稀釋之事實，或其商標之功能已被削弱，才能構成所謂商標被稀釋。

實例上，法院認為，如果於電子郵件之標題或其下之內容使用他人之商標，如「aol」 或者是「 hotmail」，而大量濫發電子郵件，已構成聯邦法中稀釋商標之行為[59]。

（4）電子通訊隱私法（Electronic Communications Privacy Act：ECPA，18U.S.C.§2701）

1986 年制定的電子通訊隱私法，是為了彌補 1968 年的竊聽法（Wiretap Act）無法因應科技發展之腳步而制定的。該法主要

[58] See Moseley et al., DBA Victor's Little Secret v. Victoria SecretCatalogue, Inc., et al., Supreme Court of the United States, Case No.01-1015 http://www.supremecourtus.gov/opinions/02pdf/01-1015.pdf (visited on 2003/8/12)

[59] *AOL v. IMS*, supra; *AOL v. LCGM*, supra; see also *Hotmail v. Van$Money Pie*, supra (court granted injunction, finding plaintiff's were likely to prevail on their federal dilution cause of action).

規範的是未獲授權或超出授權範圍，而進入電腦系統讀取儲存中之電子通訊訊息，如聲音訊息及電子郵件之行為。因此，若濫發電子郵件者未經 ISP 業者同意,擅自將其大量電子郵件儲存在 ISP 業者的電腦系統內，即違反電子通訊隱私法，若為明知或故意者，則受損害的一方可要求法院核發禁制令，及請求依實際損害以金錢賠償（如總數超過最低賠償金額一千美元）以及支付律師費用。

用戶放在ISP業者主目錄（home directory）內的檔案應被認為是屬於私人的資訊，就如同傳輸中的電子郵件信箱及通訊設備是私有財產；檔案如放在公共目錄領域時，可依所有人的判斷來檢查或修改或移除，但若有非法資料儲存在私人帳號內時，只有依法院發給的搜索令狀始可進行搜索[60]。此外，本法也禁止電子通訊服務提供者公開儲存中的通訊內容，只有以下三種情況下例外：

-已獲得該訊息發信人或收件者的授權許可；
-為通訊系統有效操作之必要；
-對政府執法單位所為之揭露[61]。

（二）現有美國州級立法

美國目前已有三十六州制定特別法規範處理濫發電子郵件之問題。 在華盛頓州與加州，因違反禁止濫發電子郵件法令而遭訴之被告，曾主張州立禁止濫發電子郵件之立法牴觸美國憲法規定，因為該立法將會使人民喪失憲法保障人民在州際間為商業行為之自由，或者使人民為州際間之商業貿易承受不當之負擔，但是顯然法院判決結果並不認同被告前述之主張，而認為該州有關禁止濫發電子郵件立法仍為有效之法律[62]。其中一個法院於其判決中更明白闡述「該種立法對於散發大量電子郵件者所帶來唯一之負擔或不便，僅是要求散佈大量郵件者應為誠實之行為，要求行為者為誠實之行為，對於州際間之商業行為並不會帶來任何負擔，並且藉由要求散佈者為誠實之行為，更可以減少詐欺之行為」[63]。

---

[60] *Typhoon, Inc. v. Kentech Enterprises*, No. CV 97-6270 JSL (AIJX) (C.D.Cal. Sept. 30, 1997).
[61] 18U.S.C.§2701；§2707；蔡淑美，＜網路廣告與消費者保護民事法律問題之研究＞，國立成功大學法律學研究所碩士論文，民國 86 年 6 月，189 頁。
[62] See *State v. Heckel*, 143 Wash. 2d 824 (2001), Supreme Court of the State of Washington www.spamlaws.com/cases/heckel.html (visited at 2003/8/2)
See *Ferguson v. Friendfinders, Inc*., 94 Cal. App. 4th 1255 (2002) Supreme Court of the State of Washington www.spamlaws.com/cases/ferguson.html (visited on 2003/8/12)。
[63] *Heckel*, supra, at 143 Wash.

在州級的立法上，通常皆較聯邦立法採取比較強硬的禁止手段（包括以刑事加以制裁違法行為人），加州就是一個最明顯的例子[64]。然而問題在於，州法的規定只能在該州的範圍內有其管轄效力，因此，只要濫發電子郵件的行為與這些州沒有管轄上的聯繫因素，就不會受到這些州法的管制。

有關截至目前美國各州已通過的管制濫發電子郵件法，請參見表 3.1　美國各州所訂立之反濫發電子郵件法律比較。

以下整理並介紹美國較著名有關禁止濫發電子郵件之州法及法院判決案例：

1.州立電腦犯罪法（*State Computer Crime Act*）

維及尼亞州電腦犯罪法（*Virginia Computer Crimes Act*）規定，意圖不法自他人取得財產上利益，未獲授權使用電腦或電腦網路者，為電腦詐欺行為之一種[65]。於*AOL v. LCGM*案件中，被告因為未獲AOL公司之授權而使用其信件系統為免費廣告之行為，被法院判定為違反維吉尼亞州電腦犯罪法。

2.州立反濫發電子郵件法（*Anti-Spam Law*）

前美國加州州長戴維斯（Gray Davis）在 2003 年 9 月 24 日簽署劃時代的反濫發電子郵件法（California Business and Professions Code Division 7, Part 3, Chapter 1 , Article 1.8. Restrictions On Unsolicited Commercial E-mail Advertisers）[66]，使人見人罵的濫發電子郵件廣告無法再進入加州電腦網路使用者的電郵信箱中。這項由民主黨籍州參議員默瑞（Kevin Murray）所提的法案規定，除非收件者明確於事前同意或其與廣告主先前有商務關係（Opt-in），禁止任何利用濫發電子郵件行銷者及其廣告商發送電子郵件給加州居民。違者將以每封電子郵件計算處以一千美元法定賠償，最高可累計到一百萬美元。包括加州在內的許多美國州政府都已完成限制濫發電子郵件的立法，但戴維斯簽署的州法卻是頭一個將濫發電子郵件發信人與廣告主一起列為約束對象的，按照這項立法，州檢察長、ISP業

[64] *California Assembly Bill 1629*(1998) Sec.502(d).
[65] See *Va. Code ss.* 18.2-152.3(3).
[66] **請參考附件七---**美國加州有關管理濫發電子郵件相關法案（California Business and Professions Code Division 7, Part 3, Chapter 1 , Article 1.8. Restrictions On Unsolicited Commercial E-mail Advertisers）

者和收件者個人都可以對濫發電子郵件的廣告商和廣告主提出民事訴訟。這個法律也是美國州法中對於濫發電子郵件管制最嚴格的法律[67]。

3.非法侵奪他人之動產（Trespass to Chattels）

大部分的州皆認為非法侵奪他人之動產（Trespass to Chattels）為普通法(Common Law)所承認之侵權行為。於CompuServe v. Cyber Promotions[68]，以及Parker v. C.N. Enterprises等案件中，對於濫發電子郵件是否為非法侵奪他人動產之行為有相當之討論，而法院實務上亦贊同ISP業者及網路使用者所提出的財產侵奪理論。

美國侵權法第二次整編§217(b)對侵奪動產的定義，為「故意使用或干涉他人對動產的持有」，而干涉則係指故意與動產引起「實質的接觸」。因此近年來美國法院判決也認為，藉由電腦產生和傳送電子訊息已足已認為是實質地接觸而構成侵奪行為。在CompuServe 一案中，被告抗辯其並未實質上剝奪原告對設備之持有，然而依照美國侵權法第二次整編§218之定義，動產之狀況、品質或價值受到損害，即是屬於侵奪動產之行為結果，該案被告因濫發電子郵件，佔據硬碟空間並損耗原告電腦設備的處理能力，導致這些資源不能用來服務CompuServe的用戶，因此，即便原告未因被告之行為受到實質上的損害，但原告的設備價值已然減損。

另外，美國侵權法第二次整編§218(d)也規定，對侵奪行為所導致損害賠償，須持有者有值得保護的法律上利益。在CompuServe v. Cyber Promotions 一案中，CompuServe主張被告發送的訊息大部分不為其用戶所需要，其用戶必須付費才能在一大堆電子郵件中找到他想要的，而用戶亦須自行付費才能自被告的郵寄名單中移除，因此許多原告的用戶抱怨這個程序不當且毫無效率，並因此而退出關閉他們在原告開立的帳號。法院判決被告行為是侵奪CompuServe之電腦系統，已損害原告對顧客的營業信譽。

---

[67] See http://news.com.com/2100-1024-5082049.html?part=dht&tag=ntop (visited on 2003/09/29)

[68] See *Compuserve v. Cyber Promotions, Inc*., 962 F. Supp. 1015 (S.D. Ohio 1997), U.S. District Court for the Southern District of Ohio www.spamlaws.com/cases/compuserve.html (visited on 2003/8/12),

綜上所述，多數州法院認為於電腦網路中傳送電子訊號已足以構成侵奪他人動產之行為，即使該行為並未侵害電腦所有人對於其電腦設備之所有權，但只要侵奪行為造成他人財產或其他價值上之減損即已足夠。至少於美國俄亥俄州（Ohio）[69]、維吉尼亞州（Virginia）[70]、加州（California）[71]、及德州（Texas）[72]，法院皆認為ISP業者可對於藉由ISP業者電腦系統及網路濫發電子郵件之人主張非法侵奪他人動產（Trespass to Chattels）。

4.不當騷擾行為（Nuisance）

於 Parker v. C.N. Enterprises 案件中，濫發電子郵件發信人使用一個不實的回信地址大量寄送電子郵件，因為所寄送郵件中大部分的收信者地址皆不存在，郵件就自動退回到不實的發送地址信箱中，使該電子郵件地址的真正使用人亦遭受到損害。除此之外，大量退回郵件亦造成 ISP 業者之損失，導致 ISP 業者之郵件伺服器暫時無法運作，而因不實發送地址而遭信件退回之電子郵件地址使用人，將喪失利用該方式通信之機會，浪費時間、甚或有可能喪失收入以及交易機會。法院認為被告（spammer）不時標示使用他人之電子郵件地址，其行為威脅原告充分使用其財產的權利，且危及網路社群的利益，並會構成對私人及公眾的騷擾。故在未經電子郵件地址所有人及管理者同意前，故意使用他人之電子郵件地址作為錯誤的回信地址，使得大量因其郵件所製造出的電子垃圾及污染都傳送到了他人的財產上，已構成普通法中之不當騷擾行為及不當侵奪他人動產之行為。

5.違約行為（Breach of Contract）

州法院也曾在判決例中認定數個濫發電子郵件發信人，已違反其與Hotmail 或其他電子郵件寄送服務提供者之契約，必須負賠償責任[73]。

---

[69] *Id.*
[70] See *AOL v. IMS,* supra, and *AOL v. LCGM,* supra (finding at Summary Judgment stage that 濫發電子郵件者s committed trespass to chattels in violation of Virginia common law);
[71] See *Hotmail v. Van$Money Pie,* supra.
[72] See *Tracey Parker, et al. v. C.N. Enterprises, et al*., District Court of Travis County, Texas, 345TH Judicial District, Case No.97-06273 http://www.loundy.com/CASES/Parker_v_CN_Enterprises.html (visited on 2003/8/12), 。
[73] *Hotmail v. Van$Money Pie,* supra ("plaintiff will likely prevail on its breach of contract claim")

6.詐欺行為及行使偽造文書行為（Fraud/Misrepresentation）

故意編造一個不實之情節或行使內容不實的文書，意圖使他人有所誤認，而陷入錯誤及受到損害，也是法院同意可以援引詐欺行為規定判定禁止的例子。在 *Hotmail* 案件聲請禁制令程序中，法院於審查時，傾向認為原告主張濫發電子郵件發信人明知其意圖違反 Hotmail 信件使用規則，但仍以不實及欺騙手段取得 Hotmail 電子郵件地址的使用權，有構成詐欺及偽造文書之可能性。

7.關於對 ISP 業者之規範

各州在對ISP業者之規範方面，加州規定ISP業者必須建立其禁止或限制濫發電子郵件的政策，ISP業者的用戶或任何人均不可以利用ISP業者的設備從事違反前述政策之行為[74]；內華達州則規定提供網際網路接取服務的ISP業者在為其使用者傳送電子郵件時，不得免除其民事賠償責任，除非其所傳送的電子郵件廣告是其自行準備或要求準備的[75]；而華盛頓州規定ISP業者等互動式電腦服務業者可以主動封鎖從其所提供服務進來的、可被合理認為有違反前述商業電子郵件傳輸規定的郵件，且不須為此確信下的封鎖負責[76]。關於有違商業電子郵件傳輸規定者，例如電子郵件訊息如果包含會讓收信者對來源產生誤解的標題（如訊息指明寄自 anyone@anywhere.com，實際上卻是從其他地方發送過來），或包含錯誤或使人誤信資訊的主旨（如主旨欄是你剛剛贏得一千元，內容卻是如何快速致富的計劃）即為適例。但是何謂ISP業者的「合理的確信」，華盛頓州州法並未對此予以具體規範，反而可能導致ISP業者濫用其檢查權而對於用戶的隱私造成侵犯。

（三）依照現有法令請求救濟之方法與範圍

1.於損害發生時先向法院取得禁制令，防免損害繼續擴大

在America Online, Inc. v. LCGM一案之簡易訴訟程序中，該案法院雖認為AOL公司主張損害額並未完成理算，所以該請求損害賠償之部分應由法院依照通常程序審理。但是，於該簡易程序

[74] *California Assembly Bill 1629* (1998) Sec.2(b)、(c)、(d)、(f)(3)(A).
[75] *Nevada Senate Bill No.13* (1997) Sec.8.
[76] *Washington House Bill 2752* (1998) Sec.6.

中，法院同意依照原告之請求，核發禁制令，禁止被告向AOL公司用戶繼續濫發電子郵件、使用aol.com系統散布電子郵件或是從AOL公司用戶中蒐集電子郵件地址。[77]

2. ISP 業者得請求之損害賠償數額

（1）依照預定可收取之廣告費用計算：

至少有一個州法院採納以ISP業者可收取之廣告費用來計算損害賠償額，即以如散佈大量郵件之行為已獲業者授權時，散佈者應支付給業者之廣告費用計算。在AOL v. Bluecard Publishing[78]案件中，被告寄送了數以萬計的大量郵件給AOL公司及其用戶，而該等郵件皆不實記載係由AOL公司所寄發。 在一個聲請一造辯論判決的案件中，法院認定被告未受他人同意侵奪他人之動產，並違反Lanham Act規定不得標示不實出處，判決被告應對於其侵權行為負責。就未受他人同意侵奪他人動產之部分，法院判決，原告得以按服務計酬之理論（quantum meruit ），請求被告支付其相當於一個廣告買主應支付給AOL 公司網頁橫幅看板(“banner advertisement”) 廣告費用，如該廣告出現在使用者之螢幕上，該費用一次約為美金$0.0055，乘以被告所寄送之郵件總數 (被告有三人，每人約寄送三千六百萬封至五千七百萬封)計算，原告可向各被告請求之金額為美金二十萬元到三十萬元元之間。而法院依據Lanham Act 之規定，認為被告之行為係故意，將損害賠償數額乘以三倍。因此，各被告應賠償之數額約為美金六十萬元至七十四萬四千元之間，並加上賠償原告支付的律師費用及其他花費[79]。

（2）依照 ISP 業者處理用戶每個郵件上所生之成本計算

在 Bluecard Publishing 案件發生之前兩年，相同的主審法官但以不同的方式計算相類似的案情損害賠償數額，該法官所審理之案件為*AOL v. IMS* 案件及 *AOL v. Prime Data Systems*[80]案

[77] *America Online, Inc. v. LCGM,* supra.

[78] See America Online, Inc. v. Bluecard Publishing, et al., U.S. District Court for the Eastern District of Virginia, Civil Action No.98-905-A http://legal.web.aol.com/decisions/dljunk/bluecardreport.pdf (visited on 2003/8/12)。

[79] “Because the matter was before the court on a motion for default judgment, based on Virginia Law, the above damages were set forth not in a Judgment but in a Report and Recommendation for Judgment, which becomes the Judgment only if no objections are made within 10 days of its service.”

[80] See America Online, Inc. v. Prime Data Systems, Inc., et al., U.S. District Court for the Eastern District of Virginia, Civil Action No.97-1652-A http://legal.web.aol.com/decisions/dljunk/primereport.html (visited on 2003/8/12),。

件。 於Prime Data 案件中，被告寄送超過一億三千封之濫發電子郵件給AOL公司及其用戶，並於郵件標上虛偽記載其郵件之來源係為 AOL公司。在聲請一造辯論判決程序中，法院認為，被告應依照侵害商標、稀釋商標、虛偽標示來源及未經他人許可侵奪他人之動產，對於原告負擔損害賠償責任，而其所據唯一計算損害賠償額之方式，係以AOL公司寄送該等信件之費用（一封約為$0.00078 元）乘以被告所寄送之郵件數量 (約為一億三千封)。依照這樣的計算方式，被告應賠償原告美金十萬一千四百元，加上對於該行為之懲罰性賠償，即將該數額以倍數計算，全部應賠償費用為美金四十萬五千元，加上原告支付的律師費用及其他花費[81] 。

在 *AOL v. IMS* 案件中，法官使用同樣的方式計算損害額，但是該案件中被告所寄送之濫發電子郵件數量較少(約六千萬)，故七個被告所應賠償之數額為美金三十一萬二千元。 法院亦注意到在兩個案件中，上述發送郵件之費用並不包括 ISP 業者的人事或是其他相關費用，而每封美金 0.00078 元之費用，事實上亦不包括 AOL 公司於此案件中實際所受到金錢上之損害。

在 1998 年，AOL公司對於某些特定向AOL公司用戶寄送大量詐欺性質電子郵件發信人提出訴訟，該等被告利用技術隱藏他們本身的身分及郵件之來源，並不理會AOL公司要求其停止行為的要求。而最後該案件於法庭上達成和解，被告同意賠償原告美金一百二十萬元，且再也不得濫發電子郵件給 AOL[82]之用戶。

同樣於 1988 年，AOL公司於其他案件中獲判一百九十萬美元之賠償及成功獲得法院所核發之禁制令。但被告並未停止其散佈大量郵件之行為，AOL向法官主張被告之行為係藐視法庭命令，因此，於 2002 年，法官判決被告應該給付原告六百九十萬美元賠償及負擔原告的律師費用[83]。

在對於 ISP 業者名譽及商譽所造成之損害方面，於 CompuServe 案件中，法院認定被告以未受他人同意侵奪他人動

[81] AOL had requested $22 million in punitive damages, but Virginia law limits punitive damages to $350,000.

[82] See AOL v. Forrest Dayton, U.S. District Court for the Eastern District of Virginia, Case No.98-1815-A. http://legal.web.aol.com/decisions/dljunk/dayton.html (visited on 2003/8/12)。

[83] See AOL v. CN Productions, U.S. District Court for the Eastern District of Virginia. http://legal.web.aol.com/decisions/dljunk/cnproductions12-2002.pdf (visited on 2003/8/12)。

產，但本案並未判決被告應賠償原告，僅核發禁制令，禁止被告為濫發電子郵件之行為。

3.聲請禁制令禁止濫發電子郵件

（1）判決前之暫時禁制令

請求法院核發禁制令，要求被告於訴訟進行中，不得再寄送大量電子郵件。

（2）於訴訟程序中向法院申請禁制令

以Hotmail v. Van$Money Pie一案為例，原告向法院提出聲請，請求於訴訟進行中，禁止被告使用任何相同或相類似Hotmail 之商標或是標示，或從事任何會使使用者混淆被告與原告商標之行為、或寄送含有不實、不具名或是錯誤之資訊、或使用任何Hotmail之電腦或電腦網路。[84]

（3）永久禁制令

禁止被告寄送、或協助他人或與他人共謀利用AOL公司之電腦或電腦網路、或寄送任何信件給 AOL公司或其用戶、或於其所寄送之電子郵件中，含有不實虛偽之資料或是錯誤之回信地址。[85]

四、美國有關反制濫發電子郵件之訴訟案例

（一）過去關於濫發電子郵件較具代表性之訴訟案例

美國在多數州管制濫發電子郵件法案尚未通過前，已有多家大型 ISP 業者對濫發電子郵件者提出訴訟，並取得禁制令或獲得賠償。以下針對具代表性的幾個重要案例加以歸納介紹。

1.Cyber Promotions, Inc. v. American Online[86]

[84] *Hotmail v. Van$Money Pie,* supra.
[85] *AOL v. Prime Data,* supra*; AOL v. IMS,* supra.
[86] See Compuserve v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997), U.S. District Court for the Southern District of Ohio www.spamlaws.com/cases/compuserve.html (visited on 2003/8/12),。

這個案件的特殊之處，在於其並非 American Online（以下簡稱 AOL）－全球規模最大的 ISP 業者－主動對濫發電子郵件者提起訴訟，而是居然由濫發電子郵件者先對 AOL 啟動訴訟，因此特具意義。

Cyber 是一家網路廣告公司，其平均每天要向 AOL 傳送一百萬份訊息給其不同的訂戶，AOL 認為 Cyber 的行徑構成了不當使用其服務系統，於是便將這些非請自來的電子郵件改變回傳路徑，反送回去給 Cyber 的 ISP 業者，導致其 ISP 業者的網路連線服務系統因大量的訊息湧入而動彈不得，Cyber 因此遭三家 ISP 業者拒絕繼續提供其所需的連線服務(有關訴訟另請詳參下述第四件案例)。Cyber 乃依美國憲法第一條修正條文之言論自由保障主張，起訴控告 AOL，而在 Cyber 提出控告後，AOL 也隨即提出反訴，主張 Cyber 濫發電子郵件給其用戶的行為，已經違反維吉尼亞州的消費者保護法、電子通訊隱私法、電腦詐欺及濫用法及維吉尼亞州電腦犯罪法。

Cyber 最初的主張有兩點：（1）在憲法第一修正案保障下其有權寄送非請自來的電子郵件；（2）AOL 運用科技裝置使用戶拒絕濫發的電子郵件是不公平競爭行為。有關第二點，法院判決認為 AOL 並沒有不公平競爭的情事；而在第一點有關憲法第一修正案的爭點上，Cyber 主張電子郵件連接到公共論壇（public forum），AOL 作為一個通到公共論壇的導引者，就如同提供公共服務，故具有國家（state actor）的地位，然而此說並不為法院所採。法院認為，網際網路既不是一項事物也不是一個地方，而只是實體存在得以流通訊息的網路，是介在虛擬和無所不在間，但任何在有關網路訟訴所稱的行為者都必須有一個提供網路連線的實體（entity），而這些實體都是私法人。

因此，就如同大部分的網路連線服務提供者，AOL 只具有私法人的地位，且連線服務提供者很少和聯邦政府有何關聯，在網路連線這個事業上也無獨占排他的壟斷地位，因此要說 AOL 具有國家的地位，實在過於牽強；此外，用戶也有權決定他們是否要接受濫發電子郵件，Cyber 也有其他傳送廣告給 AOL 用戶的管道，例如直銷信函、電話行銷、電視、印刷媒體甚至傳單等等，亦可選擇其他的 ISP 業者作為傳送電子郵件的媒介，並不會產生限制言論自由的現象，故駁回 Cyber 的訴訟。

2.AOL v. Bluecard Publishing

此案係有關濫發電子郵件發信人製造錯誤的訊息來源，導致減損 ISP 業者聲譽之判決。原告 AOL 主張，被告 Bluecard 不僅大量寄發非請自來的電子郵件，並使用科技躲過 AOL 之檢查及過濾，甚至還在其電子郵件之標頭上偽標"aol.com"，造成 AOL 之用戶誤解該信件是從原告 AOL 用戶而來；另外，被告等於不花分文便能在原告網路上刊登廣告，可說已剽竊了原告實質上的廣告收益，且被告濫發電子郵件亦妨礙了原告的電腦系統運作及商業信譽。

維吉尼亞州東區地方法院最後在本件訴訟適用類似契約關係對原告加以救濟，以合法廣告主應支付之廣告曝光率平均價格（0.0055 美元），乘以依原告所舉證被告寄發的電子郵件數量作為公平衡量損害的依據，且由於被告在被要求停止時不予理會表現出明顯輕忽法律之惡意行為，法院並依美國商標法藍哈姆法（15U.S.C. §1117 (a)）之規定，酌定三倍損害賠償額之賠償，另准予原告請求被告支付律師費用 15,646 美元[87]。

3.Parker v. C.N.Enterprises

本件原告Tracy LaQuey Parker是flowers.com網域名稱的擁有者，其並設立了一個Http://www.flowers.com的網路花藝公司，提供花藝材料的訂購及諮詢服務。被告C.N.Enterprises公司未經原告授權或明示、默示或有效同意，使用kim@flowers.com及kim!@flowers.com作為其大量寄發非請自來電子郵件的回信地址，結果則導致一些因寄自非有效地址的濫發電子郵件都退回原告處，另有些湧入的郵件則抱怨原告製造垃圾郵件，使原告蒙受實質上的損失，包括對其客戶的服務中斷、失去聯絡溝通、損失處理本事故時間、失去應有收入及失去訂約機會等損害。而被告未經原告的連線服務公司Zilker Internet Pard.Inc.的同意即耗費其電子郵件處理資源及儲存容量，並使Zilker被迫為處理數以千計突然出現的電子郵件，而無法正常運作其郵件伺服器，故Zilker便與Parker等人提出訴訟，請求法院核發禁制令，並要求被告損害賠償。另外，德州的ISP業者協會（TISPA）及EFF-Austin也代表其

[87] **See** America Online, Inc. v. Bluecard Publishing, et al., U.S. District Court for the Eastern District of Virginia, Civil Action No.98-905-A http://legal.web.aol.com/decisions/dljunk/bluecardreport.pdf (visited on 2003/8/12)。

全體會員希望取得禁止本案被告在網路上使用任何其他錯誤的回信地址，及未經ISP業者書面同意不得以其服務寄送大量電子郵件的命令。

德州TRAVIS郡地方法院法官認為，被告並無使用flowers.com作為其大量郵件回信地址的法律上權利，且被告未獲原告授權其使用該網域名稱作為錯誤的回信地址，已構成普通法上的騷擾（nuisance）及侵奪動產（trespass）。另外，法官也認為原告的網域名稱已因被告行為而價值遭到淡化，並有使原告聲譽受到永久性侵害的可能。由於這些傷害難以適當衡量及給予適當救濟，故准予核發永久禁制令。法院也進一步判決，為了避免TISPA及其會員，以及EFF-Austin及其會員將來遭受與原告相同的損害，故判令禁賠償止被告未經同意使用其他網域名稱作為大量郵件回信地址，並命被告損害[88]。

4.Cyber Promotions, Inc. v. Apex Global Information Services, Inc.

此案源於 1996 年 10 月 25 日，Apex Global Information Services, Inc.（以下簡稱AGIS）與Cyber Promotions, Inc.（以下簡稱Cyber）簽訂書面契約提供網路連線服務，到了 1997 年 3 月兩造又簽定續約。然而第二次訂約與第一次之差異在於，第二份契約禁止AGIS在未於三十日前通知的情況下終止對Cyber的服務，且確認Cyber是從事寄送大量廣告電子郵件的業者。但到了 1997 年 9 月，AGIS以受到ping攻擊[89]為由，未經事前通知，即對Cyber終止連線服務，於是Cyber便起訴向法院尋求救濟。

本件承審法官認為，即使是網路上不受歡迎的公民，如濫發電子郵件者，也有享受其契約上權利有效使用服務之權利。因為三十日前通知係兩造議定的規定，有其執行力，且ping攻擊並未超過AGIS所能合理控制範圍，AGIS也明知提供Cyber連線會有導致其系統受ping攻擊的可能性，而AGIS也曾向Cyber保證其能應付此種攻擊。另外，在AGIS終止對Cyber的連線服務後，AGIS還繼續提供連線給其他濫發電子郵件者，並也繼續受到ping的攻擊，因此AGIS拒絕提供連線服務給 Cyber並無理由[90]。

---

[88] See Tracey Parker, et al. v. C.N. Enterprises, et al., District Court of Travis County, Texas, 345TH Judicial District, Case No.97-06273 http://www.loundy.com/CASES/Parker_v_CN_Enterprises.html (visited on 2003/8/12)。

[89] Pings的設計是供網路使用者檢查其網路連線之用，有時也被不法用來癱瘓連接網路的電腦。

[90] See *Cyber Promotions, Inc. v. Apex Global Information Services, Inc.*, No. 97-5931（E.D.Pa.

（二）2002 年以來美國法院審理濫發電子郵件案件之判決

1.禁止濫發電子郵件法案之合憲性（State v. Heckel）[91]

華盛頓州對俄勒岡州（Oregon）居民 Jason Heckel 提起訴訟，因為被告寄送數以萬計之電子郵件給華盛頓州的居民(被告每星期寄送之數目約為十萬封至一百萬封，並以利用蒐集電子郵件地址之程式取得郵件地址)。該州主張被告違反華盛頓州之商業電子郵件法案，因為該信件含有不實並引人錯誤之內容，地方法院駁回該訴訟，認為州政府所訂立之法案已使州際間之商業受到阻礙，而違反美國憲法之規定。但上訴法院廢棄地方法院之判決，並認為 「該種立法對於濫發電子郵件者所帶來唯一之負擔或不便，僅是要求其應為誠實之行為，但是要求行為者為誠實之行為，對於州際間之商業行為並不會帶來任何負擔，並且藉由要求濫發電子郵件者為誠實之行為，可以減少詐欺之可能」。

為了處理濫發電子郵件所造成的傳輸困難，ISP 業者必須對於電腦設備為更多的投資，需僱用更多客服人員處理這些郵件對於用戶所造成之困擾，或僱用更多的職員來偵測濫發電子郵件之發信地址。當他人濫發電子郵件時，將會使網路使用者於使用網路時遭受使用困難而降低網路運作之效率，這種成本費用之轉換，本來應由濫發電子郵件發信人支付，但卻轉嫁至收件者，就如同寄送郵件時要求收件人付費或是打電話給他人而要求對方付費的情形相同，因此，政府對於濫發電子郵件發信人此種轉嫁成本費用之行為，自有防止其發生之必要。

另外，2002 年加州Ferguson v. Friendfinders案件被告也曾以類似理由主張加州反濫發電子郵件法案（California Business & Professions Code sec. 17,538.4 et seq., and Penal Code, sec. 502）違憲，但法院判決不採納其抗辯。[92]

2.政府對於濫發電子郵件行為所提出之訴訟

Sept. 30, 1997）

[91] See http://www.spamlaws.com/cases/heckel.html (visited on 2003/8312)

[92] See Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255 (2002) Supreme Court of the State of Washington www.spamlaws.com/cases/ferguson.html (visited on 2003/8/12), 。

2002 年在加州State of California v. Paul Willis 案件，被告濫發數以百萬計電子郵件，違反加州反濫發電子郵件法案，加州政府起訴主張法院應核發禁制令禁止該行為，並請求對於每個違反之行為命被告給付美金兩千五百元。[93]

雖然美國加州早在 1998 年即有管制濫發電子郵件法案出現，但直到 2003 年 10 月才出現首宗反濫發電子郵件廣告的判決例。這個案例是根據加州於 2003 年 9 月才剛通過的反濫發電子郵件法修正法律條文所下的判決，該法案對於濫發電子郵件者採取更嚴格的管制措施，包括允許個人用戶控告濫發電子郵件者，並訴請賠償最高可以每封電子郵件一千美元計算的損失。

加州檢察總長Bill Lockyer在 2002 年對洛杉磯濫發電子郵件者－PW Marketing，及其負責人Paul Willis及Claudia Griffin提起公訴，指控該公司在網路上濫發上百萬封廣告郵件，推銷如何發送垃圾廣告及銷售大量電子郵件地址，同時也沒有提供收件人拒絕再收該廣告的電話及電子郵件地址。加州法院於 2003 年 10 月根據上述新法判決PW Marketing公司及兩名負責人有罪，處以罰金 200 萬美元，並令其不得再上網發送未經收件人同意的商業電子郵件，不得未經許可侵入他人電腦，也不得以假電子郵件地址寄發電子郵件，同時，該兩名負責人十年內不得擁有及經營網路廣告事業[94]。

另外，密蘇里州首席檢察長 Jay Nixon 在 2003 年 10 月，亦根據密蘇里州反濫發電子郵件法對兩名濫發電子郵件者提起訴訟，這件案例亦是密蘇里州在其反濫發電子郵件法通過後首次做成之判決。

密蘇里州之反濫發電子郵件新法甫於 2003 年 8 月 28 日正式施行，該法要求所有未經收件者事前同意之商業性電子郵件須在其主旨欄上標明”ADV,“之字樣；若郵件內容涉及色情或其他與成人內容相關者，亦須於主旨欄上標明”ADV：ADLT.”之字樣。該法亦禁止發信人得悉收件者表明拒絕收信後，再繼續對收件者寄發電子郵件，否則可依每次行為處以 5000 美元，每天最多不超過

[93] See People of the State of California v. Paul Willis, et al., Superior Court of California, County of Santa Clara, Case No.CV811428 http://caag.state.ca.us/newsalerts/2002/02-111.pdf (visited on 2003/8/12)。

[94] See http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=3687808&pageNumber=0 visited on 2003/10/29）

25,000 美元之罰款。

上述案件之被告Philip Nixon因其未在寄送的電子郵件上標明"ADV,"字樣，及在收件者要求不要再寄送時仍繼續濫發電子郵件，而被密蘇里州之檢察官起訴。檢察官也請求法院下達禁制令，制止被告繼續濫發電子郵件[95]。

3.對於濫發電子郵件法案抗爭者所提出之訴訟

Moore v. Uy (2002 年馬里蘭州案件) 起因於濫發電子郵件收件者對於濫發電子郵件者提出反擊，將濫發電子郵件者之姓名及其事業內容公佈在網站上。為此，濫發電子郵件者起訴，請求法院禁止網站公佈散佈者之姓名及其事業之內容，惟其請求遭法院駁回。[96]

4.對抗濫發電子郵件發信人之法院判決

Earthlink v. Kahn案件 (2002 年 7 月) 法院判決濫發電子郵件者應賠償二億五千美元[97]。

AOL v. C.N. Productions 案件對於濫發電子郵件發信人藐視法庭之禁制令，企圖繼續其濫發電子郵件之行為，法院判決被告應賠償六百九十萬美元[98]。

Earthlink v. Carmack案件 (2003 年 5 月) 法院判決濫發電子郵件發信人因濫發八億二千五百萬封之電子郵件，被告應賠償ISP業者一千六百萬美元[99]。

5.其他進行中案件

AOL公司於 2003 年 4 月 14 日，提出五件訴訟，請求濫發電

[95]See http://news.com.com/2100-1028-5089720.html （visited on 2003/10/29）
[96] See http://news.com.com/2100-1029-996002.html (visited on 2003/8/12)
[97] See http://www.internetnews.com/IAR/article.php/1430591 (visited on 2003/8/12)
[98] See *AOL v. C.N. Productions*, (E.D. Va. 1998), http://legal.web.aol.com/decisions/dljunk/cnproductions12-2002.pdf (visited on 2003/8/12)
[99]See http://www.earthlink.net/about/press/carmack/ (visited on 2003/8/12), "EarthLink (Nasdaq: ELNK), one of the nation's leading Internet service providers, today received a $16.4 million judgment against a Buffalo, New York 濫發電子郵件者 who sent more than 825 million illegal spam emails since March 2002.U.S. "

子郵件者應賠償其八百萬美元[100]。

微軟（Microsoft）公司在 2003 年 6 月，於英國及美國提出合計十五件訴訟，向濫發電子郵件者請求損害賠償。[101]

最令人矚目的是，2003 年 12 月 18 日，紐約州檢察長史畢哲與微軟公司聯手對美國知名的濫發電子郵件之王 OptInRealBig.com 電子郵件行銷公司和委託其濫發電子廣告郵件的 Synergy6 直銷公司，分別在紐約州與華盛頓州提起民事訴訟，請求各該公司及其負責人還有受僱人連帶賠償。OptInRealBig.com 的雇員入侵 AOL 企業及個人用戶電腦系統，傳送回信地址不實的電子郵件廣告，來促銷 Synergy6 直銷公司從中抽取佣金。依紐約州檢察官調查，OptInRealBig.com 每天發出超過一億封廣告電子郵件，促銷交友服務、股票操盤服務、貸款服務及減肥藥商品等。

紐約州雖然還未有專門反制濫發電子郵件的法律，但是，州檢察長是依該州普通法規定對上述被告起訴。同時，微軟公司則是併依華盛頓州普通法與反濫發電子郵件法起訴，指控被告不法利用微軟公司電腦系統程式對 Hotmail 用戶濫發誤導及內容不實的電子郵件廣告。美國輿論咸信，這是美國近年來一連串打擊濫發電子郵件者的司法行動中最為震撼的訴訟，預期將形成先例，促使委託濫發電子郵件者與實際濫發的行為人負起連帶賠償責任。而在美國聯邦 CAN-SPAM ACT 將於 2004 年 1 月 1 日施行前夕，各州檢察長及 ISP 業者對濫發電子郵件者大張旗鼓，積極起訴的動作似乎也有消弭外界對 CAN-SPAM ACT 將來施行效果悲觀的意味。

[100]See http://www.cbsnews.com/stories/2003/04/15/tech/main549378.shtml (visited on 2003/8/12), " America Online has filed five federal lawsuits targeting 濫發電子郵件者s it accuses of sending some 1 billion junk e-mail messages promoting mortgages, steroids and pornography to its subscribers. The case resulted from about 8 million individual spam complaints from subscribers, most of whom used a "Report Spam" feature AOL introduced last fall, the company said Tuesday. The lawsuits, one filed Friday and the rest Monday in the U.S. District Court in Alexandria, Va., are the first anti-spam cases AOL launched since May 2001. They seek damages of more than $10 million plus an end to the messages."

[101] See http://www.msnbc.com/news/927809.asp, http://news.findlaw.com/hdocs/docs/microsoft/spam/ (visited on 2003/8/12).

表 3.1　美國各州所訂立之反濫發電子郵件法律比較

美國州名	必須指明商業或是色情信件	必須標示收件者得選擇拒絕收件	必須標示發信人之姓名或是地址	禁止錯誤或是不實的信件標示	限制於網頁中蒐集電子郵件地址	對於違反行為主張救濟之權利	法定賠償金額	刑事處罰規定	其他特別之規定
阿拉斯加 Alaska[102]	以ADV或ADLT指明商業廣告或是色情郵件	無	無	無	無	無	無	無	
亞利桑那 Arizona[103]	以ADV指明是商業廣告	有	標示寄件地址	有	有	有	每違反一次賠償美金十元，每日最多二萬伍千元美金	無	
阿肯色州 Arkansas[104]	無	有	須標示寄件者姓名、地址及電子郵件地址	有	有	有	違反一次賠償美金十元，每日最多二萬五千美金	可能處以重罪或輕罪之處罰（例如蓄意詐欺等）	誠實信用原則可作為抗辯

[102] *Alaska Statutes* sec. 45.50.479, http://www.spamlaws.com/state/ak.html（visited on 2003/9/18）

" **Sec. 45.50.479. Limitation on electronic mail.**

(a) A person may not send unsolicited commercial electronic mail to another person from a computer located in this state or to an electronic mail address that the sender knows is held by a resident of this state if the commercial electronic mail contains information that consists of explicit sexual material that another law provides may only be viewed, purchased, rented, leased, or held by an individual who is 18 years of age or older, unless the subject line of the advertisement contains "ADV:ADLT" as the first eight characters.

(b) In (a) of this section,

(1) "commercial electronic mail" means electronic mail consisting of advertising material for the lease, sale, rental, gift, offer, or other disposition of real property, goods, or services, including an extension of credit; (2) "explicit sexual material" means material that visually or aurally depicts conduct described in AS 11.41.455(a), but is not limited to conduct engaged in by a child under 18 years of age; (3) "unsolicited commercial electronic mail" means commercial electronic mail sent to a person who (A) does not have an existing personal or business relationship with the sender; and (B) has not given permission for or requested the sending of the commercial electronic mail.

[103] Arizona Statutes sec.44-1372 et seq.（approved 5/16/03）, http://www.spamlaws.com/state/az.html（visited on 2003/9/18）

[104] Arkansas Code sec. 4-88-601 et seq.（approved 4/2/03）, Criminal Code sec. 5-41-201（approved 4/13/01）, http://www.spamlaws.com/state/ar.html（visited on 2003/9/18）

美國州名	必須指明商業或是色情信件	必須標示收件者得選擇拒絕收件	必須標示發信人之姓名或是地址	禁止錯誤或是不實的標示	限制於網頁中蒐集電子郵件地址	對於違反行為主張救濟之權利	法定賠償金額	刑事處罰規定	其他特別之規定
加州 California[105]	無	須有先前或現存的關係	標示寄件地址	有	有	有	每次違反，賠償一百美元或一美元最高萬元之賠償	在處罰規定下，對於使用電腦詐欺或是其他相關罪責最高三年以下之有期徒刑。	美國唯二兩州採取opt-in 機制之一
科羅拉多 Colorado[106]	須標示ADV表示電子廣告郵件	有	標示寄件地址	有	有	有	無	無	
康乃迪克 Connecti-cut[107]	無	無	無	有	有	有	每次違反罰金多至五萬美元，最高一千美元	重罪或輕罪的處罰	不得散布或偽造郵件可改變路徑的軟體
德拉瓦 Delaware[108]	無	有	標示寄件地址	無	無	無	無	除非有先前存在之關係，否則濫發電子郵件行為為犯罪行為	為一強制的opt-in 法規，然目前尚未實施
愛達華 Idaho[109]	無	有	標示寄件地址	有	有	有	每次違反罰金一百美元，最高到一千美元	無	寄送非請字來的電子郵件給二人以上即構成濫發電子郵件行為

[105] *California Business & Professions Code* sec. 17,538.4 et seq., and *Penal Code*, sec. 502, http://www.spamlaws.com/state/ca1.html（visited on 2003/9/18）

[106] Colorado Revised Statutes sec. 6-2.5-101 et seq. （effective 6/3/00）http://www.spamlaws.com/state/co.html （visited on 2003/9/18）

[107] Connecticut Criminal Code sec. 53-451 (effective 10/1/99) and Civil Code sec. 52-59b (effective 1999),] http://www.soamlaws.com/state/ct.html （visited on 2003/9/18）

[108] Delaware Criminal Code sec. 931 et seq. (effective 7/2/99), http://www.spamlaws.com/state/de.html（visited on 2003/9/18）

[109] Idaho Code sec. 48-603E (effective 7/1/00), http://www.spamlaws.com/state/id.html （visited on 2003/9/18）

美國州名	必須指明或商業色情信件	必須標示者得拒絕收件	必須標示發信人之姓名或地址	禁止錯誤或不實的標示	限制於網頁中蒐集電子郵件地址	對於違反主張之權利	法定賠償金額	刑事處罰規定	其他特別之規定
伊利諾 Illinois	以ADV或ADLT指明商業廣告或是色情郵件	有	標示寄件地址	有	有	有	每違反一次賠償十美元，每日二千美金，最多五萬元	重罪或輕罪的處罰	
印第安那 Indiana[110]	以ADV或ADLT指明商業廣告或是色情郵件	有	標示寄件地址	有	有	有	每次違反罰金五百美金	無	
愛荷華 Iowa[111]	無	有	標示寄件地址	有	有	有	每次違反十百美金，最高千元五百美金	無	排除發善的自慈機構郵件
堪薩斯 Kansas[112]	以ADV或ADLT指明商業廣告或是色情郵件	有	須標示者寄件姓名、地址、電話及電子信箱地址	有	有	有	民事賠償：每次違反五百美金，須賠至一百千	無	
路易斯安納 Luisiana[113]	標示ADLT指明是色情郵件	無	無	有	無	無	無	每次五千美元之罰金	不得散布偽造可改變郵件路徑的軟體

[110] Indiana Code sec. IC 24-5-22-1 et seq. (approved 4/17/03), http://www.spamlaws.com/state/in.html （visited on 2003/9/18）

[111] Iowa Code sec. 714E.1 et seq. (effective 7/1/99), http://www.spamlaw.com/state/ia.html （visited on 2003/9/18）。

[112] Kansas Senate Bill 467 (approved 5/17/02), http://www.spamlaws.com/states/ks.html （visited on 2003/9/18）。

[113] Louisiana Revised Statutes, sec. 73.1 et seq. (effective 8/15/99), http://www.spamlaws.com/state/la.html （visited on 2003/9/18）。

美國州名	必須指明商業或是色情信件	必須標示收件者得選擇拒絕收件	必須標示發信人之姓名或是地址	禁止錯誤或是不實的標信件標示	限制於中電網頁蒐集子郵件地址	對於違反行為主張救濟之權利	法定賠償金額	刑事處罰規定	其他特別之規定
緬因 Maine[114]	以 ADV 或 ADLT 指明商業廣告或是色情信件	有	標示姓名及寄件地址	有	無	收信者	收信者得向散佈者請求每一次違反美金二百五十元之賠償。ISP 業者得向散佈者請求每一次違反美金一千元之賠償。		法律適用之門檻，必須將垃圾郵件寄送至二個收件者以上。
馬里蘭 Maryland[115]	無	無	無	有	有	有	每次違反一千美金	無	
密西根 Michigan[116]	需標示廣告郵件	有	姓名、住址，及電子郵件	有	無	收件者、ISP 業者及州政府	每次違反請求賠償金額於美金五百元以下或每天美金二十五萬元。	可能重罪之處罰；四年以下有期徒刑且得併科二萬五千元之罰金。	
明尼蘇達 Minnesota[117]	以 ADV 或 ADLT 指明商業廣告或是色情信件	有	標示寄件地址	有	有	有	每次違反為 25 美金，每天最多三萬五千元美金；若將客戶資料流出，ISP 須付每筆五百美金	無	ISP 亦須對洩漏電子郵件地址或其他個人資料負責

[114] **請參見附件八---**美國緬因州有關管理濫發電子郵件相關法案*Maine Revised Statutes*, Section 1497. http://www.spamlaws.com/state/me.html（visited on 2003/9/18）。

[115] Maryland Commercial Law Code sec. 14-3001 et seq. (enacted 2002), http://www.spamlaws.com/state/md.html （visited on 2003/9/18）

[116] **請參見附件九---**美國密西根州有關管理濫發電子郵件相關法案*Michigan Public Act 42*, House Bill 4519 (Approved July 11, 2003; effective September 1, 2003) http://www.spamlaws.com/state/mi.html（visited on 2003/9/18）

[117] Minnesota Statutes se. 325M.01 et seq. and 325F.694 et seq. (effective 3/1/03), http://www.spamlaws.com/state/mn.html (visited on 2003/9/18)

美國州名	必須指明商業或是色情信件	必須標示收件者得選擇拒絕收件	必須標示發信人之姓名或是地址	禁止錯誤或是不實的標示	限制於中電件網頁集子郵件地址	對於違反行為主張救濟之權利	法定賠償金額	刑事處罰規定	其他特別之規定
密蘇里 Missouri[118]	以ADV或ADLT指明商業廣告或是色情信件	有	標示寄件地址	有	有	有	每次違反可請求元之賠償；最高至五千萬元美金	無	
內華達 Nevada[119]	需標示廣告郵件	有	姓名、住址，及電子郵件	有	無	有	每次違反請求賠償金額五以下	可能重罪之處期徒刑且得併科十萬元之罰金。	於1997年，內華達州是第一個實行反垃圾郵件法案之州。
新墨西哥 New Maxico[120]	以ADV或ADLT指明商業廣告或是色情信件	有	標示寄件地址	無	有	有	每次違反五金，每天多美金	無	
北卡羅萊納 North Carolina[121]	無	無	無	有	有	有	每次違反美金，最多天二千金	輕罪或重罪處罰	
北柯達他 North Dakota[122]	以ADV或ADLT指明商業廣告或是色情信件	有	無	有	有	有	每次違反犯美金，最多天二千金	輕罪或重罪處罰	

[118] Missouri Revised Statutes sec. 407.1120 et seq. (effective 8/28/03), http://www.spamlaws.com/state/mo.html （visited on 2003/9/18）

[119] **請參見附件十---**美國內華達州有關管理濫發電子郵件相關法案 *Nevada Revised Statutes sec. 41.705, et seq.*, and sec. 205.492, et seq . http://www.spamlaws.com/state/nv.html（visited on 2003/9/18）

[120] New Maxico Statutes sec. 57-12-23 et seq. (approved 4/5/03), http://www.spamlaws.com/state/nm.html （visited on 2003/9/18）

[121] North Carolina General Statutes sec. 14-453 et seq. (effective 12/1/99)and sec. 1-539.2A et seq.(effective 12/1/99), http://spamlaws.com/state/nc.html （visited on 2003/9/18）

[122] North Dakota Century Code sec. 51-27-01 et seq. (approved 4/11/03), http://www.spamlaws.com/state/nc.html （visited on 2003/9/18）

美國州名	必須指明商業或是色情信件	必須標示收件者得選擇拒絕收件	必須標示發信人之姓名或是地址	禁止錯誤或是不實的標信件標示	限制於中電件網頁蒐集子郵件地址	對於違反行為主張救濟之權利	法定賠償金額	刑事處罰規定	其他特別之規定
俄亥俄 Ohio[123]	無	有	姓名、住址，及電子郵件	有	有	有	收件者求違百金萬可請次一美五元至美金；ISP業者求違十萬可請次五反美金	無	
奧克拉荷馬 Oklahoma[124]	以ADV或ADLT指明商業廣告或是色情信件	有	標示寄件地址	有	有	有	每次違元每多五美金，最萬元美天二千金	無	禁止寄送過故意或失以使人陷於錯誤、誤導的郵件而使人受到損害
奧瑞岡 Oregan[125]	以ADV指明是商業廣告信件	無	無	有	有	有	收件者或ISP可請次五一美求違每反到元，每天五百萬元美千金二千金	無	
賓夕法尼亞 Pennsylva-nia[126]	無	有	標示寄件地址	有	有	有	ISP業者求一元可請次十元，最一十美每至美金，多至五元百萬金	重罪或及二百萬元輕罪，金五一千至五美金	禁止傳真、電子郵件或其他無線傳輸工具偽造傳路徑以傳送訊息

[123] Ohio Revised Code sec.2307.64 (effective 11/1/02), http://www.spamlaws/com/state/oh.html （visited on 2003/9/18）

[124] Oklahoma Statutes sec. 776.1 et seq. (effective 11/0/02), http://www.spamlaws.com/state/ok.html （visited on 2003/9/18）

[125] Oregan Revised Statutes sec. ORS 646.607 et seq. (approved 9/17/03), http://www.spamlaws.com/state/or.html （visited on 2003/9/18）

[126] Pennsylvania Criminal Code sec. 7661(approved 12/16/02) and Trade & Commerce Code sec.2250.1 et seq. (approved 12/16/02), http://www.spamlaws.com/state/pa.htmi （visited on 2003/9/18）

美國州名	必須指明商業或是色情信件	必須標示收件者得選擇拒絕收件	必須標示發信人之姓名或地址是寄件地址	禁止錯誤或不實的標示	限制於中電件網頁集子郵件地址	對於違反行為主張救濟之權利	法定賠償金額	刑事處罰規定	其他特別之規定
羅德島 Rhode Island[127]	無	有	標示寄件地址	有	有	有	每次違反五百美元，每天最多萬美元至二千美元	五年以下有期徒刑及五千美元罰金	以電腦或入侵電腦詐騙定罪
南柯達他 South Dakota[128]	以ADV或ADLT指明商業廣告或是色情信件	無	無	有	有	有	每次違反五百元美金至一萬元美金	無	累犯可處三倍的罰金額
田納西 Tennesse-e[129]	須標明ADV指明其為廣告商業郵件	有	標明寄件地址	無	有	有	每次違反十元美金，每天最高千元美金	無	禁止散佈偽造可郵件路徑的軟體
德州 Texas[130]	以ADV或ADLT指明商業廣告或是色情信件	有	標明寄件地址	有	有	有	每次違反十元美金，每天最高萬元到二千五美金	重罪	不能販賣或散佈電子信箱用戶資料
猶他 Utah[131]	以ADV或ADLT指明商業廣告或是色情信件	有	須標明寄件者姓名、地址及郵件地址	有	有	有	每次違反十元美金，每天最高萬元到二千五美金	重罪	

[127] Rhode Island Commercial Law sec. 6-47-1 et seq. (effective 7/8/99)；Criminal Offenses sec. 11-52-1 et seq. (effective 10/1/99), http://www.spamlaws.com/state/ri.html （visited on 2003/9/18）

[128] South Dakota Statutes sec. 37-24-6 et seq. (approved 2/27/02), http://www.spamlaws.com/state/sd.html （visited on 2003/9/18）

[129] Tennessee Code sec. 47-18-2501 et seq. (effective 7/1/03), http://www.spamlaws.com/state/tn.html （visited on 2003/9/18）

[130] Texas Business & Commerce Code sec. 46.001 et seq. (effective 9/1/03), http://www.spamlaws.com/state/tx.html （visited on 2003/9/18）

[131] Utah commerce & Trade Code sec. 13-36-101 et seq. (effective 5/6/02), http://www.spamlaws.com/state/ut.html （visited on 2003/9/18）

美國州名	必須指明商業或是色情信件	必須標示收件者得選擇拒絕收件	必須標示發信人之姓名或是地址	禁止錯誤或不實是的標示	限制於網頁中電子郵件蒐集地址	對於違反主張救濟之權利	法定賠償金額	刑事處罰規定	其他特別之規定
維吉尼亞 Virginia[132]	無	無	無	有	有	收件者、ISP 業者	收件者得每次求額元每五千元。ISP 業者得每次求額元每五千元。	不佈該之過，被重以處刑。	收罪之及用腦及財產。
華盛頓 Washington[133]	無	無	無	有	無	收信者及 ISP 業者	收信者得金之請求美元賠償損害，ISP 業者得金請求美元	無	
西維吉尼亞州 West Virginia[134]	無，但是散佈色情資訊為違法之行為	無	姓名及電子信箱地址	有	無	收件者及 ISP 業者	收件者得金或違美之償日千元；每超十元賠每五萬元。	無	禁止散何圖描電子信件。

[132] **請參見附件十一---**美國維吉尼亞州有關管理濫發電子郵件相關法案*Virginia Code*, Title 18.2, Crimes and Offenses, sections 18.2-152.2, 152.3:1, 152.4, 152.12 & 152.16 (2003)http://www.spamlaws.com/state/va.html（visited on 2003/9/18）

[133] **請參見附件十二---**美國華盛頓州有關管理濫發電子郵件相關法案 *Revised Code of Washington*, Title 19, Business Regulations, sec. 19.190.010, et seq. http://www.spamlaws.com/state/wa.html（visited on 2003/9/18）

[134] **請參見附件十三---**美國西維吉尼亞州有關管理濫發電子郵件相關法案-*West Virginia Code*, Chapter 46A, Consumer Credit and Protection Act, Article 6G, Electronic Mail Protection Act, sec. 46A-6G-1, et. seq., Added by Acts 1999, chapter 119, House Bill 2627 http://www.spamlaws.com/state/wv.html (visited on 2003/9/18)

美國州名	必須指明商業或是色情信件	必須標示收件者得選擇拒絕收件	必須標示發信人之姓名或是地址	禁止錯誤或是不實的標示信件	限制於網頁中蒐集電子郵件地址	對於違反行為主張救濟之權利	法定賠償金額	刑事處罰規定	其他特別之規定
威斯康辛 Wisconsin[135]	須以ADLT指明為色情郵件	無	無	無	無	無	每求千每求上五收件者可請一千元；ISP可請以萬美金此次十或二元美金	重罪	
懷俄明 Wyoming[136]	無	無	無	有	有	有	無	無	

共同的特徵:

1. 如果發信人之住所係於某一州或該信件之寄送係經由某一州，則應適用該州之法律。
2. 未經許可使用他人之姓名或是電子信箱作為回信地址為違法。
3. 出售設計用來偽造或竄改持續發送郵件的軟體為違法行為，ISP 業者試圖阻止濫發郵件散佈之行為，免負法律責任。

[135] Wisconsin Statutes sec. 944.25 (approved 6/01/01), http://www.spamlaws.com/state/wi.html（visited on 2003/9/18）

[136] Wyoming Statutes sec. 40-12-401 (effective 7/1/03), http://www.spamlaws.com/state/wy.htnl（visited on 2003/9/18）

表 **3.2** 美國聯邦國會審查中法案之比較

法案編號	商業郵件必須標示	需給予使用者不接收濫發電子郵件之選擇 (opt-out)	必須標示發信人有效之住址	禁止錯誤或是不實的郵件標示	限制於網頁中蒐集電子郵件地址	色情郵件必需標示	對於違法行為主張救濟之權利	法定賠償金額	唯一的請求賠償依據	刑事處罰條款	其他特別之規定
H.R. 2515 [137]	有	有 --至少實施五年	有 --實際之街道地址	有	有	有	僅有ISP業者及州政府．聯邦貿易委員會亦可執行	以每件郵件賠償美金十元計算，上限為美金五十萬元，如果係故意行為，賠償金額可乘以三倍	有	有，罰金或二年以下之徒刑	
H.R. 2214 [138]	有	有 --至少實施三年	有 --街道地址	有	有 --但銀行業例外許可		僅有ISP業者及州政府.聯邦貿易委員會亦可執行	每件以賠償美金一百元計算，上限為美金一百萬元，情節重大賠償可乘以三倍	有	有。罰金及二年以下有期徒刑。	
H.R. 1933 [139]	有 --標示廣告ADV	有	有 --電子郵件即足夠	有	無	有 *--標示成人ADLT	收件者.聯邦貿易委員會亦可執行。	收件者可請求每件郵件美金十元計算之賠償及律師費用。	有，除了州立法及未或許可侵入他人動產及侵權行為之主張。	無	
S. 877 [140]	有	有	有 -有效之郵政寄送地址	有	有		ISP業者及政府相關單位。	可請求以每件郵件美金十元計算之賠償；上限為美金一百五十萬元及律師費用。	有，除了州立法及未或許可侵入他人動產及侵權行為之主張及刑事詐欺之主張。	有，罰金及一年以下有期徒刑。	

[137] *Anti-Spam Act of 2003* (53 co-sponsors)
[138] *Reduction in Distribution of Spam Act of 2003* (27 co-sponsors)
[139] *REDUCE Spam Act of 2003* (26 co-sponsors)
[140] *CAN-SPAM Act of 2003* (17 Co-sponsors)

法案編號	業件須示商郵必標	使接電之予不發件給者濫郵擇需用收子選(opt-out)	標信效址須發有住必示人之	止誤是實信標禁錯或不的件示	於中電件制頁集郵址限網蒐子地址	郵需色情必示標件	違為張利對於行主權之	賠額定金法償	的賠據一求依唯請償	處款事條刑罰	他別規其特之定
S. 1293 141	無	無	無	有	非行但成量之非的會裁期為，是為刑依據。並法	無.	ISP 業聯府者及政邦	二千賠以郵金八算金五之或件美至計美萬元償每件二元。	無	罰五下徒有，及以期金年五刑。	收犯有之部產沒與罪關全財。
S. 1231 142	，示告有標廣(ADV)	創件擇受子度絕發件制是收選收電制拒濫郵記但了得意發件有沒受子登有設者同濫郵，接電之度。	有（街址道地）	有	有	無，但送成之郵限於未者子無對給年電件制。	ISP 業州府、政關件者、邦機收政聯府及者	件賠元，收得一元反要，美千每件十算件者求美違冊時償五。以郵償計每件請千，註求賠金元。	無	無	反ISP 者政係法行。違業之策違之為
H.R. 122 143	，是止送請來告件手利電郵為同行。無但禁寄不自廣郵至機或用子件相之為	無	無	無	無.	無.	府件政收及州者	件五美算有需三每件元計亦能償。以郵百金，可賠倍	無	無	法係於止用動號話傳廣之正此案對禁使自撥電及真告修案

[141] *Criminal Spam Act of 2003* (11 co-sponsors)
[142] *Stop Pornography and Abusive Marketing Act*
[143] *Wireless Telephone Spam Protection Act*

參、日本

一、濫發電子郵件對網路使用造成的影響

日本是全世界無線通訊發展程度最先進的國家之一，日本的居民通常使用行動電話收取電子郵件，或是經由行動電話下載其所需要的資訊。因此，由電腦網路傳送至行動電話之濫發電子郵件在日本引起更多之問題與爭議。因為通訊服務的用戶(subscriber)必須付費下載傳送至行動電話之訊息，不論該訊息是否為用戶事先同意預訂，而提供傳輸服務之通訊業者則必須支付額外之費用大量增添設備及人力，來處理大量之濫發電子郵件。

根據日本規模最大之行動電話公司 NTT DoCoMo Corp. (DoCoMo)統計，在九十五億封經由該公司系統送至給客戶之訊息，超過百分之八十係隨意寄送或濫發之信件，而該公司亦花費數百萬日圓來處理退回之信件，但大部分由發信人提供之回信帳號皆為無效帳號[144]。在 2001 年 11 月，DoCoMo 取得總務省之許可，建立了一套新的機制，使行動電話使用者能在下載訊息前先觀看信件之部分內容，再決定是否下載來降低濫發電子郵件所帶來之困擾與爭議程度。

DoCoMo 同時也積極採取司法行動努力禁止濫發電子郵件之傳送，例如在 2001 年 10 月，DoCoMo 即向法院申請禁制令，禁止網站經營者 Global Networks 向字尾為"@docomo.ne.jp"的電子郵件地址濫發大量的廣告電子郵件。但是，這些個案救濟方式畢竟無法全面地遏阻層出不窮的濫發電子郵件寄送。因此， DoCoMo 動議展開立法管制濫發電子郵件的遊說行動，日本國會也正視 DoCoMo 的請求有了具體回應。

二、目前日本管制濫發電子郵件立法發展現況

針對行動電話用戶及行動電話公司受到濫發電子郵件現象的困擾，日本總務省早先於 2001 年 4 月邀請行動電話、PHS 業者提出實況調查及因應對策等相關報告，並在同年 11 月底，邀請學者、

[144] See http://www.cnni.co.uk/2003/BUSINESS/asia/03/25/docomo.reut (visited on 2003/8/12).

相關業者、消費者保護團體代表舉辦一系列研討會徵求公眾意見。經由 DoCoMo 之努力及一般大眾之支持，日本終於在 2002 年 4 月 17 日，通過兩個有關反濫發電子郵件之法案，一為特定電子郵件法（The Law for Appropriate Transmission of Specified Emails , Law No. 26 of 2002）[145]，另一是對於 1976 年特定商業交易法之修正（1976 Specific Commercial Transactions Law, Law No. 28 of 2002）[146]。以上二個法律皆於 2002 年 7 月 1 日生效，不僅規範以個人電腦收發的商業電子廣告郵件，以行動電話收發者也包括在內。

（一）特定電子郵件法

特定電子郵件法針對防止寄送大量不請自來之商業電子郵件，訂定了具體措施。該法定義應受規範的特定電子郵件為，發信人與收件者間無契約、商業往來或其他法律關係之商業電子廣告郵件，要求寄送大量不請自來郵件之發信人應標示其姓名、公司名稱、發送來源之電子郵件地址、及收件者拒收郵件時可資利用的聯絡資訊，並於信件主旨欄標示為廣告郵件：

- 在收件者未打開電子郵件前，發信人欄須有發信人電子郵件地址之記載，且主旨欄須載明「未承諾廣告※」之字樣及符號，但收件者主動訂閱之電子郵件不在此限。此項規範主要是便利於收件者判斷該郵件為廣告，並能決定是否開啟閱讀[147]。

- 在電子廣告郵件的內文中，須有發信人及業者的電子郵件地址、公司名稱及拒收廣告郵件的聯絡方法，且其提供之資料必須為真實且明確。若發信人與業者是同一人時，尚須標明「發信人＝業者」；若寄件人與業者非同一人時，則須分別於內文中標示出發信人與業者的名稱、拒收郵件的聯絡方法等等。

該法禁止發信人將電子廣告郵件寄送至隨意擷取之電子郵件地址，並提供收件者得選擇不同意收件之機制，收件者有權以明示之方式要求不得再寄送廣告郵件。如果發信人收到收信者拒絕收受之通知，不得再寄送任何垃圾郵件，經主管機關命其改正而不改正時將受五十萬日圓以下罰鍰之處罰。尤其值得注意的是，

[145] **請參考附件十四---**日本特定電子郵件法
[146] **請參考附件十五---**日本特定商業交易法修正法案
[147] 林雅慧，＜行銷策略、隱私尊重可平衡？日本如何制定「電子信件廣告法」？＞，資訊與電腦月刊，民國 92 年 5 月，46-49 頁。

本法與韓國之立法例相同，規定通訊事業提供者得拒絕提供濫發電子郵件發信人任何有關之電信服務[148]。

（二）特定商業交易法的修正

配合特定電子郵件法之立法，日本也修正特定商業交易法有關通信販賣、連鎖販賣及業務提供誘引販賣等有關直銷商品及服務之規定，增列以電子通訊方式所為直銷也受規範，以保護消費者免受不當直銷行為損害。修正條文要求，發信人應將收件者如何可以拒絕收受廣告之方法加註於電子郵件中。當發信人被收件者告知拒絕收受廣告時，即應停止繼續寄送廣告。如果收件者於受通知後仍繼續其濫發行為，收件者得向總務省提出申訴，經命改正而不改正者，可處發信人三百萬日圓以下之罰鍰甚至被追訴處二年以下之有期徒刑。

（三）消費者申訴機構

日本受理消費者對違法寄送廣告郵件業者的申訴機構，有總務省委託的「日本資料通信協會」，及經濟產業省（前「通產省」）指定的「日本產業協會」。這兩個機構除了可以針對申訴個案進行事實之調查外，亦可向委託之主管機關提出就違規業者之具體報告，並建議給予適當之處罰。原則上，對於違反「特定電子郵件法」規定之業者，消費者得向「日本資料通信協會」申訴；對於違反「特定商業交易法」規定之業者，消費者得向「日本產業協會」申訴。若消費者不明白該向哪一個機構申訴時，也可以選擇其一申訴。

「日本資料通信協會」是總務省依據特定電子郵件法第十三條規定授權，以行政命令指定，自 2002 年 7 月 10 日起開始處理申訴違反特定電子郵件法中有電子關廣告郵件之規定事項。對於業者或發信人違反應記載事項規定之申訴，申訴人須檢附收到該郵件之日期、發信人之電子郵件地址、郵件名稱、原始的郵件內容，並且附上申訴人之真實姓名、電子郵件地址、所使用的電子郵件服務業者名稱；對違反再送信之禁止規定者(即已告知發信人拒絕再收到此類商業廣告，但仍收到該廣告時)，申訴人須具名檢附最初收到的郵件內容、申訴人已表示拒絕再收到該廣告而業者仍繼續寄發廣告郵件內容的紀錄，提出申訴。

[148] See http://www.law.duke.edu/journals/dltr/articles/2002dltr0021.html. (visited on 2003/8/12).

「日本產業協會」則是經濟產業省依特定商業交易法第六十一條規定授權，以行政命令指定，處理申訴違反特定商業交易法中有關廣告電子郵件規定之事項。依該協會之說明，申訴業者及發信人違反應記載事項之規定者，申訴人須提出收到日期、發信人的電子郵件地址及內文內容。對於違反再送信之禁止規定者，申訴人應檢附其原先收到廣告內容之紀錄、收件人前已發出拒絕再收到該業者廣告郵件之意思表示，以及仍繼續收到業者寄來的廣告郵件內容之紀錄。

三、日本民間業者對抗濫發電子郵件之行動

配合上述新法施行，日本相關電信公司也積極引進新的技術，建立保護其用戶免受濫發電子郵件侵擾之機制。例如，DoCoMo 提供其用戶選擇阻擋任何標題標明為廣告之電子郵件。同時，DoCoMo 公司及另一家日本主要的行動電話公司 KDDI 也聯手建立起新的措施防止發信人藉由行動電話網路濫發電子郵件。如有用戶向電話公司提出抱怨，電話公司將追蹤該濫發電子郵件來源，並暫時停止對於該發信人之服務。如果濫發電子郵件之情況並無改善，電話公司繼續接到其他用戶之申訴，電話公司將立即終止對於該客戶之服務，並停止該發信人所有登記行動電話之服務。

這樣的積極行動也擴展到具體的個案申訴救濟上。在 2003 年 3 月 25 日，DoCoMo贏得日本第一個對抗濫發電子郵件發信人之案件。一家日本公司因經常透過DoCoMo行動電話網路濫發大量廣告色情郵件至DoCoMo用戶手機，DoCoMo起訴請求禁止及賠償，法院判決該公司應賠償 DoCoMo日圓六百五十七萬元。[149]

肆、大韓民國

一、濫發電子郵件問題對網路使用造成的影響

大韓民國(以下簡稱韓國)是世界上網路使用者數目成長最快的國家。根據韓國網路資訊中心(KRNIC)[150]2003 年 7 月發表的報告，韓國使用網際網路的人數於 2001 年 12 月已增加到二千四百三十八

[149] See http://security.itworld.com/4774/030711imodespam/pfindex.html (visited on 2003/8/12)
[150] See http://isis.nic.or.kr (visited on 2003/8/12).

萬人，而在 2002 年 12 月人數則到達二千六百三十萬人，成長速度非常驚人。 使用網際網路服務而以電子郵件作為通訊的人口也以相同的高速增加，從 2001 年 12 月到 2002 年 12 月，已大幅增加至百分之七十六點五。[151]這個現象與韓國快速普及寬頻網路建設展現具體成效有直接的正向關聯。

在網際網路及電子郵件使用率大幅增加之同時，濫發電子郵件變成一個無法避免之問題。根據韓國資訊安全局(Korea Information Security Agency， KISA)[152]的調查，網路使用者申訴受到濫發電子郵件侵擾之數量逐年以倍數成長:

年份	2000	2001	2002	2003	
				一月	二月
申訴件數	325	2923	106076	7470	8224

(來源: 韓國資訊安全局，2003 年 3 月)

至今，韓國已變成亞洲最努力與濫發電子郵件對抗的國家。韓國是亞洲最先立法禁止濫發電子郵件的國家，並將原本法律所無法涵蓋之漏洞以修法之方式加以補上。

二、目前韓國管制濫發電子郵件立法之發展現況

韓國政府在 2001 年制定資訊、通訊、網路利用及資訊保護法（ Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 ）。本法將「濫發電子郵件」定義為大量傳輸招攬生意商業廣告之電子郵件，採用「事後拒絕」(Opt-out) 之機制，規定如收件者明示其不願意繼續收受商業廣告，則發信人不得繼續發送廣告。

資訊及通信院作為本法規定事項之主管機關訂定相關施行細則（Ordinance of the Ministry of Information and Communication of the Act)，要求電子商業廣告郵件發信人將 “ADV”等字樣標示於電子郵件之標題上，並強制所有藉由網際網路寄送電子商業廣告郵件者，應標示其電子郵件之主題內容、發信人之姓名及其聯絡方式，還有收件者不願意繼續收受此種郵件時，其可以利用之

[151] See http://security.itworld.com/4774/030711imodespam/pfindex.html (visited on 2003/8/12)
[152] See http://www.kisa.or.kr (visited on 2003/8/12).

方式。依本法規定違反上述強制或禁止規定者可處高達五百萬韓元之罰金(約相當於美金 4,1523 元)。

儘管如此，濫發電子郵件現象並不曾稍有歇息，鑽取法規漏洞迴避管制的事例層出不窮，甚至與日本之情形相似，加速向行動電話網路蔓延。韓國政府決定更加嚴格執行反濫發電子郵件措施，進一步修正了資訊、通訊、網路利用及資訊保護法（The Revised Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 ），於 2002 年 12 月 18 日公佈，2003 年 1 月 19 日施行。資訊及通信院原所發佈之施行細則，亦隨著新法之公布而加以修正。2003 年 1 月 24 日，韓國資訊安全局隨即設立新的申訴處理中心 Korea Spam Response Center，專責處理受害的收件者申訴，進行先期調查確認，一經認定申訴內容屬實，則由該中心具名向檢警機關及資訊及通信院提出正式檢舉，請求究辦。該中心亦負責打擊濫發電子郵件活動的推廣與相關國際合作。

新法將濫發電子郵件定義為「任何經由電話、傳真、或是其他經由政府所公告之媒體，傳送經收件者明示拒絕收受之商業廣告」。新的定義使得反濫發電子郵件法律不僅可適用於法律公佈時原定之傳輸方式，並包括任何於該法施行時可能不存在之傳輸方式 (例如行動電話)。從 2003 年 6 月 19 日起，所有利用行動電話網路寄送廣告者亦須標示「廣告」之字樣、廣告之內容及發信人聯絡之方式。

新法規定，發信人必須嚴格遵守標示電子廣告郵件之規則，不得將廣告之標示，如 ADV 變更為「 “A*D*V”」 或「 “A~D~V”」，而電子郵件中包含僅限成人閱覽或色情之內容時，必須標示 “ADULT”字樣。違反前述法規濫發電子郵件之發信人將面臨最高額提高到一千萬韓元之罰金處罰。

新法仍維持事後拒絕機制（Opt-out）[153]。如果收件者已經明示拒絕收受任何郵件廣告，發信人即不得繼續寄送。發信人並須負責證明其有提供正確之聯絡方式，也未曾以任何技術方法規避收件者向其表達拒絕繼續收受郵件之通知。 除此之外，發信人必

[153] As there have been increasing concerns with respect to the effectiveness of opt-out scheme, the Korean government is currently reviewing the possibility of enacting an opt-in regime in an attempt to further tighten the enforcement of anti-spam regulations（採考慮採取事後拒絕之方式可能無法達到預期的成效，韓國政府已經在考慮以事前同意之方式取代。）

須提供收件者得拒絕收信之機制，且不得向收件者收取額外之費用[154]。

又參照未成年人保護法（Minor Protection Act）相關規定，新法明定任何寄送給未滿十九歲未成年人之廣告，不得含有有害於未成年者之內容，[155]違反者可依未成年人保護法追訴刑事有期徒刑之處罰。新法也禁止使用以軟體程式自動蒐集他人電子郵件地址、或與他人分享、交換、買賣或提供從網路上所獲取的電子郵件地址。[156]

濫發電子郵件對於ISP業者當然是一個頭痛問題，實務上，ISP業者在給濫發電子郵件發信人多次書面通知或電話通知催告改正後，發信人仍不停止其行為時，ISP業者即會對其停止提供服務。但是，這樣的實踐曾經產生法律上的爭議。新法增加規定，如 ISP

[154] **Article 50 (Restrictions on Transmission of Advertisement Information)**
(1) Any person shall be prohibited from transmitting advertisement information for the purpose of soliciting business against the addressee's explicit rejection of such information.
(2) Any person who intends to transmit by email, telephone, facsimile, or other media prescribed by Presidential Decree any advertisement information for the purpose of soliciting business under paragraph (1) shall expressly indicate the matters falling under each of the following subparagraphs in the advertisement information under the conditions as prescribed by Presidential Decree:
1. The types of transmission information and major contents thereof;
2. The name and contact means of the addressor;
3. The source of email address harvested (pertinent to email spam); and
4. Matters concerning easy methods to reject receipt of future advertisement information.
(3) It shall prohibit senders of advertisement information for the purpose of soliciting business from performing any technical manipulation so as to avoid denying further reception.
(4) Senders of advertisement information for the purpose of soliciting business shall perform necessary management prescribed under Presidential Decree so that recipients do not expenses the fees caused by indicating their intention not to receive any further advertisement.
(5) No one shall transmit advertisement information for the purpose of soliciting business by using software or other technical equipment that generate contacts by collating with numbers, codes, or characters.

[155] **2 of Article 42 (Prohibition of the Advertising "Media Materials Harmful to Minor")** Providers of information and communications services shall be prohibited from transmitting to minors, under subparagraph 1 of Article 2 of the *Minor Protection Act*, advertisement implying media materials harmful to minor described in subparagraph 4 of Article 7 of the *Minor Protection Act*, which are prescribed as harmful to minors in accordance with subparagraph 3 of Article 2 of the same Act, via email, telephone, facsimile, or other media prescribed by Presidential Decree.

[156] **2 of Article 50 (Prohibition of the Harvesting Email Addresses from Websites, etc.)**
(1) No person shall harvest email addresses from web pages that expressly prohibit automatic harvesting of email addresses with software or other equipment.
(2) No person shall sell or circulate email addresses in violation of paragraph (1).
(3) No person shall knowingly use email addresses that had been automatically harvested for the purpose of sale or exchange as stipulated by paragraph (1) or (2) regarding transmission of advertisement information.

業者認定發信人有濫發電子郵件之行為，或有合理之懷疑，且雙方所訂定之服務提供契約約定對於濫發電子郵件之行為，ISP業者有權停止對其提供服務時，ISP業者即可停止提供其服務。[157]

新法自 2003 年 1 月施行六個月以來，本法主管機關資訊及通信院一共對二十三個濫發電子郵件發信人(大部分是網路商店或線上遊戲業者)處以四百萬及五百萬韓元不等的罰金。這些發信人都是對於收件者拒絕繼續接收廣告郵件請求置之不理，而受處分。另外，有二百七十個濫發電子郵件發信人，因為不遵守規定在廣告郵件主旨標題明示其性質為廣告，而受到主管機關警告。資訊及通信院表示，如果濫發電子郵件現象再無改善，將對繼續發現的違法情形處以法定最高限額一千萬韓元的罰金。

韓國政府代表在 2002 年 10 月於漢城主辦亞洲隱私保護論壇(Asia Privacy Forum)開幕演說中聲明，該國政府已經正確認知到防制濫發電子郵件，不能夠僅靠立法手段解決，而仍需要社會普遍參與及網路使用者的充分配合。韓國資訊安全局（Korea Information Security Agency , KISA）於是著手利用公開教育的方式，使社會大眾皆能了解濫發電子郵件問題之嚴重性。這個大型的宣導教育計劃包括，舉辦推廣落實反濫發電子郵件法案之活動，發行反濫發電子郵件指導原則給ISP業者及主要的電子商務業者，指導業者學會尊重消費者隱私，鼓勵業者自發參與提醒公眾了解隱私權保護的重要性以及必要做法，以求徹底解決濫發電子郵件的問題。韓國資訊安全局並且已經開發出一套軟體，藉由使用該軟體，可以將收件者電子郵件地址不以真實姓名及其他特徵表示，使濫發電子郵件發信人使用自動寄發裝置無法認出電子郵件地址。這個軟體稱為“Never Spam”（不要濫發），任何人都可以免費在 Korea Spam Response Center 網站 http://www.spamcop.or.kr 下載取得。[158]

韓國資訊安全局也繼續推動修法，希望強制所有電子廣告郵件

---

[157] **4 of Article 50 (Restrictions of Service for Transmitting Advertisement)**

(1) ISPs may deny certain services at their own discretion where there is or will be obstruction caused by repetitive transmission spam, or if users do not want to receive such information.

(2) Where ISPs intend to deny certain services under paragraph (1), they shall indicate matters of their right of denial in their contract.

(3) Where ISPs intend to deny certain services under paragraph (1), they shall give notice to the user of that service or persons having an interest.

[158] **請參見附件十六---** *“Anti-Spam Regulations in Korea”* by Dr. Hyu-Bong Chung, Ph.D (2003/03/28)http://www.privacy.org.nz/media/Chung.pdf (visited on 2003/8/12)。

在標題上標示 “@”符號，取代現行法所規定 “ADV”字樣。韓國資訊安全局表示，這樣做法有助於所有國家不論其使用語言文字有何差異，在發展過濾濫發電子郵件軟體程式時，只要設定以 “@”符號來辨識進行過濾，就可以減少因各國立法管制規定歧異可能的漏網之魚。韓國政府聲稱，即使短期內上無法達成全球共識，統一上述過濾記號，但是，各國網路使用者無論身處何處，將來只要在過濾軟體程式中設定“@” ，至少可以阻擋絕大部分來自韓國的濫發電子郵件。韓國政府強調，這是韓國作為世界公民，為網際網路秩序維持所盡的一份心力，並以此積極推動國際合作，目前已經分別與香港及澳洲達成合作備忘錄的簽署。

三、韓國民間業者對抗濫發電子郵件之行動

韓國最大的入口網站業者 Daum Communications Corp.,針對日益泛濫的濫發電子郵件現象，尋求以市場及科技的解決方案雙管齊下，在實質上減少濫發電子郵件的數量，於 2002 年 4 月 1 日啟用所謂的「線上戳記系統」。

Daum Communications 分析，濫發電子郵件發送的成本相當低，但是，發信人或廣告主所獲得的效益卻是非常驚人。只要有一個收件者願意採購濫發電子郵件內所廣告之商品或服務，就足以使發信人或廣告主回收其發送費用。但相對而言，ISP 業者以及網路使用者，所要負擔的成本卻顯然遠遠高於發信人。該公司研究以為，將廣告郵件之發送費用由發信人轉嫁給全體收件者分擔，不僅是不合理，並且與市場經濟原理相違背。為了矯正這樣不合理之狀況，又不阻礙合法商業者經營者使用網路資源，該公司創設出如下圖 3.1 所示的「線上戳記系統」:

線上戳記系統對於寄送大量電子郵件者先註冊，並且建立寄送大量電子郵件之價目表，Daum Communications 對於電子郵件經線上戳記系統加以註記者保證送達至收件者，線上戳記系統同時則進行線上的意見調查，鼓勵用戶檢舉濫發電子郵件，對於主動檢舉或回覆意見調查的收件者給予記點回饋獎勵(rewards)。依照 Daum Communications 之內部報告指出，啟用該線上戳記系統以後有效減少了大量電子郵件不斷重複傳送造成之網路壅塞情況，收件者對於濫發電子郵件之申訴件數也有減少的傾向。

Daum Communications 也發現，透過藉由線上戳記系統註冊後所發送之電子郵件，內容往往較為豐富，因此獲得收件者正面回應歡迎的比例也更加提高。

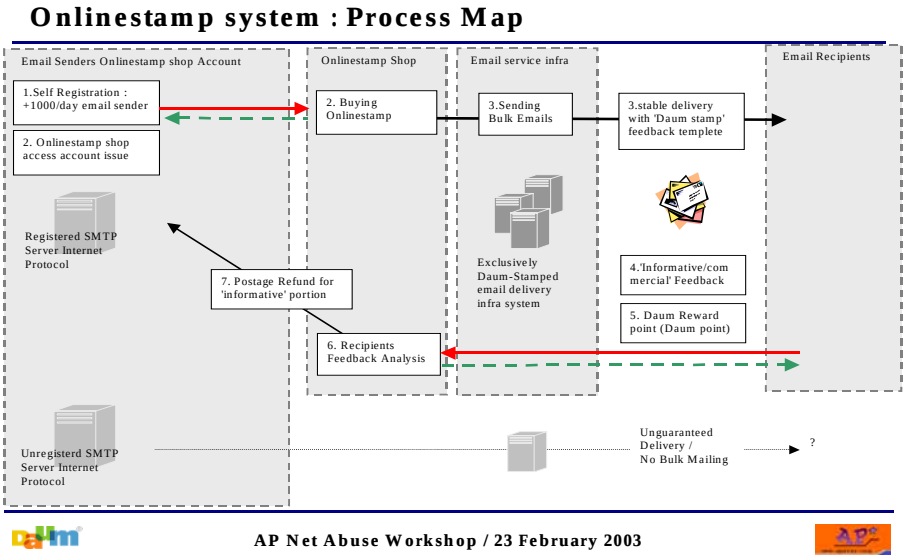


圖 3.1 「線上戳記系統」

另外，值得注意的是，在韓國修正資訊、通訊、網路利用及資訊保護法加重對濫發電子郵件發信人之處罰後，Daum Communications 於 2003 年 6 月對四家開發及散佈濫發電子郵件軟體程式的公司，向漢城地方法院檢察署提出刑事告訴。同時，該公司也同步對該四家公司向法院聲請民事假處分，請求禁止設計、銷售、散佈及使用上述濫發電子郵件軟體程式。這是韓國史上第一次由民間業者針對濫發電子郵件行為提出的訴訟，也因此格外引起各方關注訴訟結果對於韓國政府及民間協力對抗濫發電子郵件行動將產生的影響。

伍、新加坡

一、濫發電子郵件對網路使用造成的影響

就如同其他科技進步之國家所遭遇情形，近幾年來濫發電子郵件在新加坡亦已大量繁殖增生。新加坡通訊主管機關 IDA 調查統計，光只在 2000 年一個年度，新加坡每個 ISP 業者每月平均收到超過 2000 件對於濫發電子郵件之抱怨。其中百分之八十以上

的申訴，係針對由新加坡以外國家所寄出之濫發電子郵件所做。

二、目前新加坡管制濫發電子郵件立法之發展現況

新加坡目前並無限制濫發電子郵件之法令。儘管在新加坡濫發電子郵件並不是非法之行為，但是濫發電子郵件所散佈之內容若含有色情的成份，或是違反了新加坡濫用電腦法第七章之規定（*Computer Misuse Act*）[159]，仍會受到主政當局依其他有關法令追訴及處罰因此，濫發電子郵件之行為在內容方面還是受到相當程度的規範。

新加坡通訊事業的獨立監理機關資訊通訊發展局（The Infocomm Development Authority , IDA）自 2002 年起對於濫發電子郵件之情形及其他各國對於濫發電子郵件之立法加以評估，考慮是否以立法之方式，宣告濫發電子郵件之行為是非法之行為。由新加坡政府協助民間企業(成員包括知名外商銀行、信用卡組織、國際大型會計師事務所、物流公司、大型入口網站業者及消費者保護團體代表)所成立,目的在促進電子商務消費者信賴關係之信任委員會（ National Trust Council, NTC），接受IDA委託研究做成結論認為，新加坡應該僅在於無法利用其他的方式遏阻濫發電子郵件時，才應考慮以法律來制止這種行為。NTC認為，相關立法工作茲事體大，而且其過程將會產生龐大費用，況且截至目前為止，各國已制定反濫發電子郵件法案之經驗尚未證明是遏止濫發電子郵件最有效之方法[160]。新加坡政府工商發展部門也疑懼立法管制濫發電子郵件可能反而有礙線上交易及網路商業之發展，而不願積極支持立法來禁止濫發電子郵件之散佈。

---

[159] **S. 7 Unauthorized Obstruction of Use of Computer**

(1) Any person who, knowingly and without authority or lawful excuse,
   (a) Interferes with, or interrupts or obstructs the lawful use of, a computer; or,
   (b) Impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

   shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[160] See National Trust Council Website at http://www.trustsg.org.sg/anti_spam.htm (visited on 2003/8/13).

三、新加坡民間業者對抗濫發電子郵件之行動

新加坡政府尚無意於制定法令來禁止濫發電子郵件，其國內相關產業就朝向以業者自律方式試圖減少及解決濫發電子郵件之問題。

（一）ISP 業者對抗濫發電子郵件之行動

網路使用者對付擾人的濫發電子郵件，除了自行加裝使用反濫發電子郵件軟體之外，最常使用的手段即是向其網路接取服務提供者提出抱怨。因此，新加坡大多數的 ISP 業者已於使用政策及受理使用者註冊程序中，規定禁止濫發電子郵件。而 ISP 業者最常使用的方式，就是當連續收到兩件以上對特定來源濫發電子郵件之申訴時，ISP 業者會寄送警告信函給濫發電子郵件之信箱所有人，警告其立即停止濫發電子郵件。如果於 ISP 業者寄送警告信函後，發信人仍不停止其散佈行為，ISP 業者會關閉該電子郵件信箱限制其繼續使用。

（二）私人企業自律實施保護個人資料之規定

新加坡的電子商務經營者以及相關利用網際網路為行銷工具的私人企業也受新加坡政府鼓勵自發實施保護個人資料模範準則（Model Data Protection Code）[161]。這份業界自律規範是由IDA及NTC所共同建立及推動，透過引入經濟合作發展組織（Organization for Economic Cooperation and Development）所訂定電子商務消費者保護指導原則[162]促使業界團體自行遵從視實

[161] A copy of the Model Data Protection Code can be obtained at the website of National Trust Council at http://www.trustsg.org.sg/model_data.htm (visited on 2003/8/13).

[162] The 10 principles are prescribed in the Model Code as follow:

- **Principle 1 – Accountability**: *An organization is responsible for personal data in its possession or custody*.
- **Principle 2 – Specifying Purposes**: *The purposes for which personal data are collected shall be specified by the organization*.
- **Principle 3 – Consent**: *The knowledge and consent of the individual are required for the collection, use, or disclosure of personal data to a third party, except otherwise prescribed by law*.
- **Principle 4 – Limiting Collection**: *Except as provided by law, the collection of personal data shall be limited to that which is necessary for the purposes specified by the organization. Data shall be collected by fair and lawful means*.
- **Principle 5 – Limiting Use, Disclosure, and Retention**: *Except as provided by law, personal data shall not be used or disclosed to a third party for purposes other than those for which it was collected, unless the individual consents to such use or disclosure*.
- **Principle 6 – Accuracy**: *Personal data shall be as accurate, complete, and*

際狀況調整出兼顧企業發展電子商務需求以及確保電子商務消費者個人資料受到適當程序措施保障不致遭濫用。這個準則並無強制性，企業得自行選擇是否實行。

這個準則與濫發電子郵件有關之部分，是因應濫發電子郵件所產生之個人資料維護安全性問題。例如，以技術或機器自動撥號或產生電子信箱帳號等等行為，皆在建議排除使用之列。依照準則第 4.3 條之規定，如要蒐集、使用、或揭露個人資料都需要得到該特定個人之同意；業者使用 cookies 蒐集及利用網路使用者個人資料的同時，應告知該使用者且得到其明示或默示之同意。在準則中亦建議，業者要建立收件者拒絕/退出接受郵件之機制，讓使用者得隨時撤銷其接受之同意表示。

陸、中國

一、濫發電子郵件對網路使用造成的影響

根據中國互聯網絡信息中心(CNNIC)統計資料顯示，中國到 2003 年 7 月為止，有為數高達 7800 萬名網路使用者，其所使用各項網路服務中，電子郵件服務以 91.8%的比例在排名上高高居首。CNNIC 有關濫發電子郵件泛濫的現象調查同時發現，在 2002 年 12 月每人每週平均收到的正常郵件數爲 7.7 封，另有 8.3 封為濫發電子郵件，相較於 2003 年 7 月的統計，網路使用者每人每週收到的正常電子郵件數減少爲 7.2 封，濫發電子郵件數目則增加爲 8.9 封。

中國互聯網協會反垃圾郵件小組 2003 年最近的調查顯示，在

---

up-to-date as is necessary for the purposes for which it is to be used.

- **Principle 7 – Safeguards**: *Personal data shall be protected by appropriate security safeguards*.
- **Principle 8 – Openness**: *An organization shall make readily available information about its policies and procedures for handling personal data*.
- **Principle 9 – Individual Access and Correction**: *Subject to the exceptions as prescribed by law, an individual shall upon his or her request be informed of the existence, use, and disclosure of his or her personal data and shall be given access to that data. An individual shall be able to challenge the accuracy and completeness of his personal data and have them amended as appropriate. The reasons for denying access should be provided to the individual upon request.*
- **Principle 10 – Challenging Compliance**: *An individual shall be able to address a challenge concerning compliance with the above principles to the designated person or persons accountable for the organization's compliance*.

中國每年約 1500 億封電子郵件中有將近三分之一為濫發電子郵件，其國內擁有郵件伺服器的企業普遍受到濫發電子郵件的侵擾，有的企業每周收到上萬封濫發電子郵件，有的企業每年爲應付濫發電子郵件投入人民幣上百萬元的設備和大量的人力，給企業造成了沈重的負擔。在數量龐大的濫發電子郵件中，有相當大部分是向網路使用者推銷他人的電子郵件地址，這就有可能使得一部分網路使用者加入到濫發電子郵件的大軍中，使濫發電子郵件的數量越來越多[163]。

二、目前中國管制濫發電子郵件立法之發展現況

中國到目前為止並沒有立法明訂規範濫發電子郵件，但是在 2003 年 9 月由中國互聯網協會召開的第七屆電子商務大會中，已經提出了「電子商務法律法規建議草案」，建議中國政府立法管制電子商務交易及手機簡訊，其中電子商務有關法律草案規定，產品不實可無條件退貨，而手機簡訊立法草案則建議必須登記用戶身份，並禁止有害內容簡訊的傳播。

令人矚目的是，在對抗濫發電子郵件的行動方面，與會的專家及政府部門代表都建議應儘速進行反濫發電子郵件立法。其中專家建言結論倡言，對濫發電子郵件發信人不僅要規定刑事責任、行政責任，而且還要規定民事責任，例如對受害者給予金錢賠償、公開賠禮道歉等。不過，也有法律專家指出，打擊濫發電子郵件不能走向另一個極端，對以寄發電子郵件爲手段進行合法的營銷活動，還是要提供合理的發展空間。政府部門代表對於有關反濫發電子郵件立法，則更關注將來反濫發電子郵件的主管部門、確定濫發電子郵件的明確定義、技術判定標準以及確定ISP的法律責任等方面[164]。

三、中國民間業者對抗濫發電子郵件所採取之行動

中國的網路郵件服務業者亦開始發起建立反濫發電子郵件協調機制。在 2002 年 11 月時，由中國互聯網協會、263 網路集團和新浪共同發起的「中國互聯網協會反垃圾郵件協調小組」在北

[163] http://www.cert.org.cn/articles/news/common/2003090121038.shtml （visited on 2003/11/06）
[164] http://it.sohu.com/59/65/article213126559.shtml (visited on 2003/9/29)

京正式成立。

「中國互聯網協會反垃圾郵件協調小組」主要任務是倡導電子郵件服務提供商及全體網路使用者共同行動起來，反對發送、轉發濫發的電子郵件，建立和完善中國的反濫發電子郵件機制，共同研究和推廣技術和管理解決方案，同時積極開展與國際上有關反濫發電子郵件組織的交流與合作，以共同抵制濫發電子郵件問題。中國互聯網協會表示，其已積極協調 263 網路集團、新浪等國內主要電子郵件服務提供商就反濫發電子郵件的管理、技術、個人行爲等方面進行深入協商與研討，共同制定和實施反濫發電子郵件的相關措施[165]。

首先，在 2003 年 11 月 20 日，「中國互聯網協會反垃圾郵件協調小組」，繼先前於同年 8 月中國互聯網協會發布「垃圾郵件伺服器名單」，接續公佈第二期名單，呼籲被列入名單的電子郵件地址所有人主動與協調小組聯繫，針對各自狀況採取相應處理措施，以停止濫發電子郵件。對於未回應協調小組呼籲也未停止濫發電子郵件的郵件伺服器，則自 2003 年 12 月 25 日零時起，由協調小組全體成員採取一致行動，對名單上的郵件伺服器電子郵件地址實施封堵過濾措施，拒收由這些伺服器發送出來的郵件。「中國互聯網協會反垃圾郵件協調小組」宣佈，其將定期更新和公佈其認定的「垃圾郵件伺服器名單」，聯合小組成員採取過濾行動。

柒、澳洲

一、 濫發電子郵件對網路使用造成的影響

澳洲統計局(Australian Bureau of Statistics)在其每年執行的資訊科技商業應用調查中揭露，澳洲企業連網普及率在 2002 年 6 月達到 72%，與 1998 年同期比較成長 167%，而 1991 年所有連網企業中有 26%是利用網際網路作為主要推廣其商品與服務的工具。相應於這樣的快速商業應用發展，以澳洲為總部的民間反濫發電子郵件聯盟(Coalition Against Unsolicited Bulk Email 簡稱 CAUBE)在 1999/2000 年的實證調查中推斷，全球濫發電子郵件中

[165] 見http://aspam.isc.org.cn/ (visited on 2003/09/29)

有 16%源自澳洲;後續的追蹤調查則顯示，濫發電子郵件源自澳洲的比例逐年遞減，由東歐及亞洲地區取代了澳洲的排名。AC Nielson 顧問公司受澳洲政府委託，在 2002 年對澳洲 ISP 業者所做調查結果顯示了相類似的觀察:濫發電子郵件仍有七成以上源自美國，但是在大型 ISP 業者方面的數據則透露，每天平均仍有 20%的濫發電子郵件是由澳洲發出。相對於此，本研究輯錄澳洲一家主要設計濫發電子郵件過濾軟體的公司 Messagecare 在 2003 年 6 月所做市場調查發現，在澳洲網路使用者所收到的大量濫發電子郵件只有 0.5%是自澳洲本地寄送，其餘都是來自境外。另外，AC Nielson 在前述 2002 年發表的報告中也指出六家大型澳洲 ISP 業者每月遭到濫發電子郵件佔用的頻寬最少在 1GB 以上，多者甚至達到 100GB。假設一般一封電子郵件要佔用 5,000 位元，濫發電子郵件佔用 1GB 頻寬換算下來等於是二十萬封電子郵件，而全部受調查 ISP 業者反映其處理之濫發電子郵件內容以色情及快速致富秘訣等兩類即已佔全部的濫發電子郵件件數八成以上，情況不可謂不嚴重。

二、 澳洲民間業者對抗濫發電子郵件所採取之行動

澳洲的法令以往對濫發電子郵件的規範相當寬鬆與模糊，因此在抗制濫發電子郵件的問題上，澳洲民間業者只能依靠自行設計網際網路接取服務契約約束網路使用者濫發電子郵件的行為以及訂立業者間行為準則予以規範。在 1996 年 2 月，澳洲網路產業協會（Internet Industry Association，簡稱 IIA）在網路上公佈了一份「網路產業自律規範」（Internet Industry Code of Practice）草案，以對網路產業面臨之諸多使用管理問題提供一個業者共同遵守的準則。

其中，在有關電子郵件行銷及消費者保護的需求上，IIA 在最近新修正的上述規範中，特別於第 10.7 條規定，除非有以下情形，否則電子商務交易商不得寄送非請自來的電子郵件：（1）與收件人先前曾存有商業、專業或私人的關係，或（2）先前曾獲得收件人表示同意隨時收受電子郵件，例如曾經在網站上表示願接受寄送郵件或相關訊息等。另外又於第 10.8 條中規定，發信者於前述兩種情形寄送電子郵件時，必須還要承諾提供下列兩種作為：（1）提供收件人於收受非請自來電子郵件時，可要求不願再收受之方法；（2）除非收件人嗣後要求，否則於收到不願再收受之要求時，即不可再寄送非請自來的電子郵件。而在第 10.10 條中也有規定，簽署此規範的電子商務交易商，不可再寄送含有被禁止傳送或非

法內容的非請自來電子郵件。

而在有關ISP業者的相關規範方面，第 10.11 條建議ISP業者最好能在用戶契約訂定禁止其用戶寄發非請自來電子郵件，或提供任何依賴非請自來電子郵件的內容或服務的約款，並且明定違背該約款之效力；第 10.12 條亦建議，ISP業者宜能提供將濫發非請自來電子郵件行為通知相關ISP業者檢查及執行的辦法；第 10.13 條規定，ISP業者最好能在其郵件伺服器安裝轉寄保護措施，使寄發非請自來電子郵件者不能掩飾發信來源或逃避檢查[166]。

三、澳洲目前管制濫發電子郵件立法之發展現況

澳洲聯邦參議員 Richard Alston 兼內閣成員通訊、資訊科技暨藝術部部長在 2002 年 2 月要求該國 National Office for the Information Economy(NOIE)針對濫發電子郵件現象及其可能之防治措施進行研究。NOIE 在 2003 年 4 月完成的調查報告結論具體建議澳洲政府立法管制濫發電子郵件(UCE)，採納事前同意機制(Opt-in)，採擷相關產業組織已經建立的自律規範內容，對於違法行為設定罰則。該報告同時也呼籲澳洲政府積極擴大國際合作共同遏止濫發電子郵件現象滋生。

在 2003 年 9 月 19 日，澳洲政府通訊、資訊科技暨藝術部由部長Richard Alston領銜提出 “A Bill for an Act about spam ,and for related purpose”(以下簡稱 Spam Bill 2003)[167]，同年 11 月 28 日於眾議院(House of Representatives)中通過。

Spam Bill 2003 明定以澳洲的電信主管機關澳洲通訊署(Australian Communications Authority，簡稱 ACA)為新法執行的主管機關,凡是具有下列任一個與澳洲關連因素(Australia Link)的商業電子訊息(commercial electronic message)發送都須受新法規範:

(1)訊息發送地在澳洲;

(2)發送訊息的個人或組織在訊息發送時現實身處澳洲或是其核心控制經營地點是在澳洲;

(3)接收訊息的電腦、伺服器或類似裝置是在澳洲;

---

[166] see http://www.iia.net.au/Code6.html (visited on 2003/09/30)；蔡淑美，＜網路廣告與消費者保護民事法律問題之研究＞，國立成功大學法研所碩士論文，民國八十九年六月，177-178 頁。

[167] **請參見附件十八---**澳洲有關管理濫發電子郵件相關法案*Spam Bill 2003* (A Bill for an Act about Spam, and for Related Purposes)

(4)該訊息收件人於收閱訊息時身處澳洲或是其為法人或非法人團體之情形其業務或活動是發生在澳洲;甚至
(5)在該訊息因收件者之電子郵件信箱不復存在而無法寄達時，只要該預定收件的電子郵件信箱可以合理推斷出在澳洲可以利用電腦、伺服器或類似裝置接取，均屬之。

值得注意的是，上述所謂商業電子訊息也包括行動電話手機接收到的不請自來簡訊(ACA 和澳洲行動電話持照者先前已經在 2003 年 6 月共同推動業者自律方案以有效減少濫以手機簡訊進行商業廣告宣傳的行為) 。但是透過一般的電話服務傳送的語音訊息則不在此限。

新法採納了事前同意原則(Opt-in)，所有上述商業電子訊息發送前須有各該收件者事前同意接受，並且發信人要在每一則訊息明示其詳細且確實之聯絡資料，還有以明確方式告知收件者回覆訊息的效果與隨後拒絕再收受相同或類似訊息的方式。在此所謂事前同意，包括事前明示同意或是藉著之前已存在的商業關係或其他關係（如親屬、朋友等）來推論已有默示同意。所謂商業電子訊息，包括內容為廣告或促銷商品、服務、土地或商業投資機會的一切電子訊息，也包括協助他人用欺騙或不實手段取得第三人財產利益的情形。但是，新法對於上述事前同意原則以及有關商業電子訊息的定義都保留另依法律授權的行政命令發布變更其範圍的權力。與歐盟 2002/58/EC (*Directive on Privacy and Electronic Communications*) 新指令所規定相同的是，政府公文書或政治性、宗教性、慈善、文化及教育機構所發送不屬商業性質的電子訊息，並不是新法規範對象。

違反新法規定的罰則包含警告、禁制令、法院判令罰金等一系列的制裁手段，罰金部分最高每天可處 110 萬元澳幣（大約相當於 81 萬 1,100 美元）。但是，過失行為則不在處罰之列。除非取得者或使用者能證明其並無濫發電子郵件之意圖，新法亦禁止提供、取得或使用郵件地址蒐集軟體；或甚且提供、取得或使用透過郵件地址蒐集軟體所製作之電子郵件名錄。

澳洲通訊署（ACA）作為新法的主管機關有權向聯邦法院提出禁制令之聲請，以限制違反本法規定的行為人從事違法行為（限制性禁制令）或命違法行為人為一定行為（執行性禁制令）。任何有意依新法規定發送商業電子訊息或從事提供、取得或使用郵件地址蒐集軟體的個人或組織可以洽主管機關簽定有執行力的承諾書

(enforceable undertakings)具體約明其承諾遵守事項，若有違反，主管機關得向澳洲聯邦法院請求發給命令，命令立書人：(1)履行承諾書內容之行為；(2)繳交相當於違反承諾所得直接及間接利益之金額與聯邦政府；(3)賠償他人因立書人違背承諾所受之損害；聯邦法院也有權採取其他適當措施。另外，在民事賠償的部分，新法規定，聯邦法院作為違反本法所生訴訟之管轄法院，聯邦法院得命被告賠償受害者損失或將被告所得利益歸由政府受領。若被告多次違反且經聯邦法院命其賠償，聯邦法院尚可考量提高被告之賠償額度。

澳洲政府在推動新法立法時強調，對於合法利用電子郵件進行直銷推廣的企業組織只要遵守澳洲隱私權保護法案(Privacy Act)規定，無須多慮新法實施會衝擊其營業。但是，澳洲直銷協會(Australian Direct Marketing Association)則憂心新法可能將嚴重打擊依賴電子郵件行銷為其主要市場推廣手段的中小規模企業。因此，新法規定，企業將有 120 天的寬限期，以調整改變其作業方式。新法預定將在 2004 年 4 月 11 日施行。National Office for the Information Economy(NOIE)也將自 2004 年開始，展開為期 12 個月針對新法內容及反制濫發電子郵件具體作為，向企業及網路使用者宣導的活動。

澳洲積極的立法作為使它成為全世界第一個以中央制定反制濫發電子郵件專法的國家[168]。但是澳洲政府更熱切呼籲國際社會，包括國際組織、各個主權國家以及民間企業、反對濫發電子郵件志工團體聯合努力對抗濫發電子郵件所形成國際性的網路災難[169]。

捌、歐盟

一、濫發電子郵件對網路使用造成的影響

根據歐盟自行統計資料，濫發電子郵件情形日益泛濫，對於電子商務和資訊社會的發展造成了嚴重問題。光是在 2002 年濫發電子郵件增加了網路使用者清理電子郵件信箱的時間和金錢支出，就造成了全歐盟生產力損失估計達 25 億歐元。歐盟執委會還

[168] 見http://taiwan.cnet.com/news/ec/story/0,2000022589,20083568,00.htm (visited on 2003/10/01)

[169] See http://www.worldebusinesslawreport.com/index.cfm?selectedpub=1,8&action=dsp_item&id=2397&xprint=1 (2003/10/29)

在 2003 年 11 月發表預測，未來數月之內濫發電子郵件將吞噬全球電子郵件流量的 50%[170]。其中，法國網路使用者每年因接收濫發電子郵件而支付的網路使用費高達數億歐元，整個歐洲則達上百億歐元。法國丘比特市場調查公司(Jupiter)2003 年第四季發佈的調查報告說，如果不加遏制，到 2007 年歐洲人民接收的濫發電子郵件數量將比現在增加 4·5 倍，屆時濫發電子郵件問題將給社會帶來更大的損失。由此可知，管理濫發電子郵件已成爲從政府到個人都無法迴避的問題。許多法國人將此歸罪於外國，根據在法國和比利時進行的一項調查顯示，這兩個法語國家民眾接收到的濫發電子郵件有 85%是來自國外的英語郵件，其中三分之一來自美國。法國輿論界因此幾乎將美國看成了濫發電子郵件的源頭。“都是美國惹的禍”，這是法國媒體在評論濫發郵件問題時經常的提法[171]。

二、歐盟目前管制濫發電子郵件法制之發展現況

歐洲議會一直在積極創造一個清晰的法律政策，使其會員國內民眾及企業組織能便利使用電信資源，兼顧不同利益間應有之平衡。在相關電信法規中由歐洲議會所提出的主要議題之一，即是有關個人資料之保護，包括針對不請自來之商業電子訊息寄送問題著手進行解決方案的規劃。

為處理電信科技快速發展所產生威脅個人隱私權的問題，歐洲議會首先於 1997 年 12 月 15 日通過一個專門處理不請自來商業電子訊息之指令:「電信部門下之個人資料處理及隱私權保護指令」[172]（Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, December 15, 1997，以下簡稱 Directive 97/66/EC或Directive on Data Protection）。

依照該指令第十二條之規定(Article 12 of the Directive

[170] see http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/world/2003-07/21/content_986328.htm （visited on 2003/11/06）

[171] see http://it.sohu.com/95/06/article215140695.shtml （visited on 2003/11/06）

[172] **請參見附件十九---**歐盟 97/66/EC電信部門下個人資料處理及隱私權保護指令 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.

97/66/EC)[173]，會員國應立法強制只有在用戶事前同意之情形才可以利用自動撥號功能的語音電話或是傳真進行直銷(for the purpose of direct marketing)。至於針對其他為直銷目的不請自來之商業通訊，會員國得選擇以下任一種機制：一是該通訊僅可發送給事前同意接受該通訊之收件者，即「事前同意」（Opt-in）機制，另一種是允許業者直接大量發送商業性質通訊給任何用戶，惟一旦用戶或收件者表示不願意接受該通訊時，發信人則不得繼續發送，即「事後拒絕」（Opt-out）機制。但是，本條規定僅適用於收件者為自然人之情況，而不適用於法人，因為一般認為法人的經濟條件及地位可以使自己在實際環境中受到較好之保護，不需要特別立法保障。

隨著電信及資訊科技快速商用化的腳步，歐洲議會認知到利用電子通訊在提升產品及服務品質方面之絕對潛力。但是，歐洲議會也了解因市場行銷所大量寄送之商業電子訊息將會產生相當多之社會問題。2000 年 6 月 8 日歐洲議會制定「資訊社會各項應用服務中內國市場電子商務之法律議題指令」[174]（On Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market , June 8, 2000，以下簡稱 Directive 2000/31/EC 或 Directive on Electronic Commerce）以為確保各會員國推動電子商務之際可以在充分保障個人資料安全的前提下自由跨境流通傳遞個人資料。在2000/31/EC指令的前言第十四項，歐洲議會言明在網際網路現實的開放架構中所存在種種匿名效應，例如濫發電子郵件，並非此指令規範所欲處理之問題，但是，歐洲議會認為，該指令可以作為歐盟會員國凡准許濫發電子郵件散佈者，在進行管制時參酌之

[173] **Article 12 Unsolicited Calls**

(1) The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

(2) Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing, by means other than those referred to in paragraph 1, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, the choice between these options to be determined by national legislation.

(3) The rights conferred by paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited calls are sufficiently protected.

[174] **請參見附件二十---**歐盟 2000/31/EC資訊社會各種應用服務中內國市場有關電子商務之法律議題指令 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce (Directive on Electronic Commerce)

指導原則。根據 2000/31/EC[175]指令第七條之規定，大量不請自來商業電子郵件發信人必須清楚標示該郵件為廣告郵件，並且提供收件者得選擇拒絕繼續收件之機制（即事後拒絕機制）。

如前所述，濫發電子郵件的問題並未於 97/66/EC指令中加以討論。當濫發電子郵件的問題益加嚴重時，歐洲議會試圖找出適當之方式來控制濫發電子郵件情形。經過多次之辯論，歐洲議會多數成員在解決方案上抱持的態度由禁止散佈濫發電子郵件轉變為採取強制取得收件人同意之機制，即「事前同意」（Opt-in）機制，發信人僅可將電子郵件送給明示同意收件者。新指令Directive 2002/58/EC [176]「電子通訊中個人資料處理及保護個人隱私指令」（Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, July 12, 2003），於 2002 年 5 月正式通過，並於 2002 年 7 月 12 日施行，會員國必須於 2003 年 10 月底前依指令具體實踐至其內國法律。

新的 2002/58/EC指令 (Directive on Privacy and Electronic Communications) 取代了 97/66/EC 指令 (Directive on Data Protection) ，事實上是加強保護各種通訊服務的用戶 (“subscribers” of communications service) ，而加重對商業組織採取直銷行為的限制。細觀其中儘管有一部份限制規定保護對象僅及於自然人用戶，而不包括法人用戶(詳參下述) 。但是，歐盟指令是對同一事項提供各會員國一個最低的執行標準，各會員國在這標準之上有權決定採取更高的要求，或擴大其保護範圍，也因此有關法人用戶就新指令規定事項在歐盟各會員國能享有的保障程度將有程度上的差異。值得特別一提的是，根據新的 2002/58/EC[177]指令規定，2000/31/EC「資訊社會各項應用服務中

[175] **Article 7 Unsolicited Commercial Communication**
(1) In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.
(2) Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

[176] **請參見附件二十一---**歐盟 2002/58/EC電子通訊下之個人資料處理及保護個人隱私指令 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communica- tions Sector (Directive on Electronic Communications).

[177] Preamble §45 of *Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* states that:

內國市場電子商務之法律議題指令」在不牴觸新指令範圍內仍為有效且繼續施行。

根據 Directive 2002/58/EC (Directive on Privacy and Electronic Communications)第十三條之規定[178]，不僅是濫發電子郵件行為強制適用事前同意機制，其它使用自動撥號系統撥打不請自來的語音電話、傳真及手機簡訊廣告者，發話方應於打電話前取得受話者之同意。在管制濫發電子郵件之部分，如果發信人之傳送郵件係因之前對收件者銷售產品或服務而取得其包括電子郵件地址在內的相關聯絡資訊，則發信人可針對相類似產品或服務之資訊再次寄送廣告郵件給收件者，而不須取得收件者事前之同意。但是，發信人應讓收件者有選擇不同意繼續收受該等廣告之權利，且不應使收件人行使該拒絕收件之意思表示因而須負擔額外費用。至於使用其他方式傳送直銷為目的之信件或是通訊，會員國得選擇收件者「事前同意」或是「事後拒絕」之機制具體規範於其內國法律中。但不論是採取「事前同意」或是「事後拒

---

§45 This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 On Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market* (Directive on Electronic Commerce) are fully applicable.

[178] **Art. 13 Unsolicited Communications**

（1） The use of automated calling systems without human intervention (automatic calling machines) facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

（2） Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

（3） Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

（4） In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

（5） Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

絕」之方式，發信人皆不得隱藏其真實身分或是標寫錯誤之回覆地址。值得注意的是，本條規定與前述 97/66/EC指令第十二條之規定相類同，只適用於收件者為自然人。

另外，歐盟執委會對於廣受矚目的網路迸出式廣告(pop-up ads)做成書面解釋(answer to Written Question E-3392/02) ，認為網路迸出式廣告在收件者離線時就會自動消失，不會儲存在收件者的終端裝置中，而認定不屬於新指令第十三條所定義的電子郵件，因此其寄送不適用事前同意原則的限制。

綜上所述，歐盟立法對於直銷行為所做限制，並非規定在單獨的特定指令以供窺其完整立場，反而是分別在先後不同的指令中劃定各個最低標準，由各會員國斟酌其內國狀況，另行訂定法令以實施於其內國市場。

歐盟執委會負責企業與資訊化社會事務的委員 Erkki Liikanen 強調，各國政府必須趕在濫發電子郵件摧毀全球使用者對於網際網路及行動通信網路的信心之前，全面對濫發電子郵件者宣戰。他代表歐盟提出對於管制濫發電子郵件問題的新計劃。該計劃將加強下列三項措施，以具體回應日漸嚴重的濫發電子郵件問題：

- 加強各國政府的執行力
- 加強國際間企業合作，例如發展郵件過濾軟體的技術及遵循法規加強管理事項的合作
- 增進公眾對濫發電子郵件問題之自我保護意識

Erkki Liikanen對國際合作的訴求更是積極，其認為由於歐盟境內接收到的濫發電子郵件多半來自於境外諸如美國及亞洲等地區，促成越多國家制定相類似管理濫發電子郵件的法令，國際合作的成效就越能彰顯。2003 年 12 月 10 日至 12 月 12 日，由聯合國教科文組織與國際電信聯盟在聯合國歐洲總部日內瓦舉辦全球資訊社會高峰會議(World Summit on the Information Society, WSIS) ，應歐盟要求在議程中特別規劃了全球防堵濫發電子郵件的國際合作議題; 接著在 2004 年 2 月，經濟合作發展組織(Organization for Economic Cooperation and Development) 將在比利時的布魯塞爾舉辦一個有關全球合作立法減少濫發電子郵件的工作會議，由Erkki Liikanen及美國FTC代表共同主持，共同

研討如何進一步透過國際合作來解決濫發電子郵件問題[179]。

三、歐盟會員實施歐盟指令之情況

歐盟指令對於歐盟之所有會員國皆有拘束的效力，但是，也提供會員國得選擇最適合其內國法之指令加以實施。當指令實施後，歐盟會指定一個期限，要求所有的會員國應於期限內增立符合該指令內容之新法或是修正既存之法律使其涵蓋與符合該指令之內容。針對有關隱私權及電子通訊之指令（*Directive on Privacy and Electronic Communications*），歐洲議會要求歐盟所有的會員國於 2003 年 10 月底前完成修正及增補立法。換言之，在 2003 年 10 月後，歐盟所有 15 個會員國，包括奧地利、比利時、丹麥、芬蘭、法國、德國、希臘、愛爾蘭、義大利、盧森堡、荷蘭、匈牙利、西班牙、瑞典及英國，都必須依新指令所規定的事前同意原則完成相關管制濫發電子郵件的立法工作。截至 2003 年 12 月 11 日，已經有奧地利、丹麥、愛爾蘭、義大利、西班牙及英國等六個會員國完成指令規定的配合實施立法工作，歐盟對於其他九個會員國也已發出通知，要求在兩個月內提出說明及限時完成。本研究謹就所研究期間內所蒐集歐盟各國相關之立法情況詳細陳述如下：

（一）奧地利

奧地利於 1999 年修正電信法（the Telecommunication Act），對於不請自來之通信（communication）， 採取收件者事前同意之規範[180]。 值得注意的是，奧地利政府除禁止散佈以行銷為目的之郵件(UCE)外，亦禁止散佈大量郵件(UBE)，違反者可處罰歐元三萬六千三百三十元以下之罰鍰。

---

[179] See http://www.worldebusinesslawreport.com/index.cfm?selectedpub=1,8&action=dsp_item&id=2458&keyword=Liikanen%20sets%20out%20further%20EU%20anti-spam%20measures (visited on 2003/11/25)

[180] The Amendments to the *Telecommunications Act* (1999-07-19) (Unofficial Translation)

§ 101 Unsolicited Calls

Calls – including the sending of telefaxes – for advertising purposes without the prior consent of the subscriber are not permitted. The consent of any one person authorized by the subscriber to use that subscriber's connection is of equal standing. Consent can be revoked at any time; the revocation of such consent has no effect on contractual relations with the party to whom consent had been given. Sending of email in bulk or for advertising purposes requires the prior – revocable at any time – consent of the recipient.

在 2003 年，奧地利再次修正電信法，以符合歐盟在 2003/58/EC 指令中之規定。在新修正條文中，擴張了原適用範圍，只要是利用自動系統或其他類似科技散發的電子郵件、傳真、電話、簡訊等等，都包含在新法規範範圍內。而對於所謂散發「大量」郵件中對於「大量」的定義，除非發信者與收信者間有先前商業關係存在，新法將其件數限縮至五十封。另外，在管制濫發電子郵件之部分，如果發信人之傳送郵件係因之前對收件者銷售產品或服務而取得其包括電子郵件地址在內的相關聯絡資訊，則發信人可針對相類似產品或服務之資訊再次寄送廣告郵件給收件者，而不須取得收件者事前之同意。但是，發信人應讓收件者有選擇不同意繼續收受該等廣告之權利，且不應使收件人行使該拒絕收件之意思表示因而須負擔額外費用。新法中也規定，若發信人沒有在郵件中表明自己寄送郵件的目的，或隱藏自己的連絡及識別資訊時，禁止其發送具有商業目的的電子郵件。

（二）比利時

2003 年 3 月前，比利時法令僅禁止傳送所有不請自來之傳真，並無任何法令規範有關不請自來之電話及電子郵件。在 2003 年 3 月 11 日，比利時國會制定有關資訊化社會應用服務之相關法律（the Law on Certain Legal Aspects of Information Society Service），落實歐盟 2000/31/EC 指令內容，並於 2003 年 3 月 27 日開始實施。

在新法第十三條規定，於一般情形下，所有用於直銷之訊息(不論其形式為何，包括透過公眾傳輸系統傳遞且能在收件端集結並下載之任何文字、聲音、影像等等，因此可包含所有來自聊天室、視訊會議、網路電話會議、文字訊息及手機簡訊之不請自來的廣告)，在外觀皆須清楚標示其為廣告文件，並且記明發信人之聯絡資料(不論係個人或是機構)，這些資料包括：（1）發信人之個人名字或公司名稱；（2）地址；（3）電子郵件地址；（4）商業登記及營業稅籍編號。發信人提供的商品及服務資訊必須附上清楚的價錢標示，特別是這些價錢是否包含稅金或郵寄費用在內，更須特別標示出來[181]。第十四條規定採取「事前同意」機制，除非事前取得收件者之同意，寄送以直銷為目的之電子郵件係違法之

[181] See http://www.internationallawoffice.com/Ld.cfm?i=59163&Newsletters_Ref=7478（visited on 2003/10/22）

行為，並且規定發信人必須在電子郵件內容中，標明收件者如何能通知發信人拒絕收件之方式及之發信人有效的回覆地址。

2003 年 10 月，比利時國會議員 Senator PhilippeMahoux 及 Senator Jean-Francois Istasse 共同提案修正上述法律以擴張納入寄送迸出式廣告(pop- up ads)電子郵件也需要嚴格地先取得收件者事前同意

（三）丹麥

丹麥早已立法採取事前同意機制來限制濫發電子郵件之散佈。在實踐歐盟 97/66/EC指令方面，丹麥於 2000 年 7 月之行銷規範法 （Marketing Practices Act）[182]將以行銷為目的之電子郵件，與自動電話廣告系統及傳真皆列為不請自來之通信而依事前同意原則限制其散佈。

第一個依照前述法律所為之刑事處罰案件於2003年5月判決:丹麥商事法庭對於一家寄送 156 封垃圾電子郵件及傳真之軟體公司加以處罰。雖然被告辯稱該等郵件係由國外寄送至丹麥，但是法院認為伺服器主機的位置是否在丹麥國內，並非本案應考慮的要點，只要是一家丹麥公司濫發電子郵件給在丹麥之收件者[183]，即應受該法之規範。

歐盟新的「電子通訊中個人資料處理及保護個人隱私指令」(Directive 2002/58/EC)於 2003 年 7 月生效施行，丹麥也已經相應完成修法納入該指令規定。

[182] **S. 6a Unsolicited Calls to Certain Customers**

(1) Where a supplier sells goods, immovable or movable property or work or services to customers, he shall not be allowed to make calls to anybody using electronic mail, automated calling systems (automatic calling machines) or facsimile machines (fax) for the purposes of such selling unless the particular customer has made a prior request for such calls.

(2) Without regard to subsection (1), at supplier having received a customer's electronic address in connection with sale of a good or a service may market his own similar goods or services to that customer electronically. This implies, however, that the customer can easily and with no extra charge object to this, both when handling over his mail address to the supplier and by subsequent calls.

[183] See www.fs.dk/index-uk.htm (visited on 2003/8/16)

（四）芬蘭

芬蘭於 1999 年修正其資料安全保護法（ *Data Security Act* ），採取「事前同意」制度 （Opt-in model）。本法禁止非經收件者事前同意寄送不請自來之廣告郵件給個人（自然人）或是新聞團體之行為;從歐盟會員國濫發電子郵件至芬蘭亦是違法之行為。新的修正法案則已經在國會審議，將落實歐盟在 2002/58/EC 指令中之規定。

（五）法國

除了依照Directive 97/66/EC指令於 2001 年所實施的法案之外，法國並沒有其他處理濫發電子郵件之立法。法國政府內閣曾於 2002 年 11 月 18 日向眾議院提出新法案，該法案之目的係將歐盟 2002/58/EC有關隱私權及電子通訊指令中之規定轉化為法國內國法。這個法案於 2003 年 2 月 26 日由眾議院一讀修正部分條文通過，刻正於眾議院等待二讀中。該法案第十二條規定，也採取了事前同意機制。據主管機關工業部表示，該法案的規範範圍含括所有以直銷（direct marketing）為目的，而以電子方式傳送廣告之行為；不過，個人間傳送訊息的行為並不包括在內。此外，處理及接受民眾對於濫發電子郵件申訴的個人資料處理及自由維護委員會（National Commission on Data Processing and Freedoms）亦表示會要求ISP業者監控濫發電子郵件的流量及有關反種族仇恨的相關訊息[184]。

（六）德國

德國目前對於濫發電子郵件尚無特別立法加以管制。根據實施歐盟指令所訂立之相關法令，任何使用電信方式所為之傳輸皆需取得收件人之同意。但是，電子郵件是否為依「電信方式所為之傳輸」，則需由法院在具體個案上來決定。

對於應該採用「事前同意」(opt-in)或是「事後拒絕」(opt-out)的制度，在德國曾產生爭議，商業人士主張如於寄送電子廣告郵件前皆須獲得收件人之事前同意，事實上會阻礙商業之發展。有

[184] See http://newsobserver.com/24hour/technology/story/782597p-5609931c.html （visited on 2003/10/29）

些法律實務界人士則認為德國既無專門之立法，受濫發電子郵件困擾的人僅能依照傳統既存之法律或法理（如未經授權進入他人動產理論或是毀損）向發信人主張侵權行為損害賠償。

在 2003 年 7 月 21 日時，德國消費者保護部門（Germany's Consumer Protection Department）主席，發表聲明表示德國將會對於濫發電子郵件採取積極對抗之行動，並期待於 2003 年底制定法案處理濫發電子郵件之問題。這個新立法提案將採取「事前同意」制，禁止任何人於得到收件人同意前，寄送商業性電子郵件，並賦予政府機關權力，監督並阻止濫發電子郵件寄送，在特定情形政府並將有權對發信人課取因濫發電子郵件所獲得之利益[185]。

（七）希臘

就處理濫發電子郵件之問題，希臘正在制定法律採取「事前同意」（Opt-in）制度，未獲收件者之同意，不得寄送或傳送以行銷為目的之電話、傳真或是電子郵件。

（八）愛爾蘭

愛爾蘭於 2003 年 2 月 24 日依照歐盟 2000/31/EC 指令，制定實施加入歐盟應配合履行的有關規定（European Communities Regulations 2003）。這個規定的目標係將 2000/31/EC指令中有關電子商務之原則加入。但是，該規定係採取事後拒絕之機制（Opt-out ），寄送廣告郵件之發信人必須於信件之標題標示其為廣告郵件，而且必須於信件中標明可供收件者聯絡之方式及資訊[186]。

但是，配合歐盟 2002/58/EC 指令明白要求歐盟會員於 2003 年 10 月底之前，對於濫發電子郵件管理採取「事前同意」（Opt-in）機制，愛爾蘭上述規定也已有相對應之修正。

[185] See http://news.yam.com/afp/color/news/200307/20030722003501.html (visited on 2003/8/16)

[186] **請參見附件二十二---**Arthur Cox Tech Brief Technology Group Bulletin, March/April 2003 http://www.arthurcox.ie/dynamic/publications/Techbrief%20-%20March-April%202003.pdf (visited on 2003/8/13)

（九）義大利

截至目前為止，義大利有三個不同之法律處理到濫發電子郵件之議題。法案 DL975/1996 規定，事業經營者應於利用個人資料時，取得該個人之同意。法案 DL171/1998 將發信人之義務擴大，規定任何經由自動系統寄送之廣告郵件，皆須取得收件者之事前同意。1999 年 5 月 22 日，義大利政府訂定實施歐盟 97/7/EC 指令有關遠距銷售之規定，施行 DL185/1999 法案，正式採取「事前同意」（Opt-in）制度。對於遭受濫發電子郵件騷擾之收件者，可以要求發信人說明其為何濫發電子郵件，如果發信人事前曾取得收信者之同意，亦必須於五個工作日內回覆，如果收件者對於發信人之解釋無法滿意時，收件者得將該情形報告義大利隱私權保護機關（ Italian Privacy Authority），經調查違法事證屬實，發信人可被處歐元五千元以下之罰鍰。

在義大利最新的修法動態中，義大利資料保護機關（Italian Data Protection Authority）剛於 2003 年 9 月 1 日起實施一項更嚴格的法規：任何未受收件者事先且明確的同意而寄送電子郵件者都是違法，最高可處歐元九千元以下之罰鍰，情節嚴重者，發信人並可能面臨三年以下之有期徒刑刑事處罰[187]。企業或個人若想以電子郵件擴展商業範圍而不違反上述法規，必須符合以下幾點規則：

(1)在寄送任何廣告電子郵件之前皆須得到收件者的同意；
(2)確定所有的郵件都必須包含發信人完整的聯絡資訊；
(3)在所有電子郵件中收件者都必須有機會保護自己的隱私權（如：取消同意之權利、要求寄件來源的資訊等等）；
(4)確定所有被列在名單或電子資料庫上的收件者都是來自已經得到收件者願意接收電子郵件廣告及進一步資訊之同意[188]。

（十）盧森堡

電子商務法（ Law Related to Electronic Commerce[189]）於

[187] See http://news.bbc.co.uk/1/hi/technology/3120628.stm (visited on 2003/9/29)
[188] See http://www.worldebusinesslawreport.com/index.cfm?action=login&c=59163&id=2344, (visited on 2003/10/15)
[189] See http://www.etat.lu/OLAS/docs/comelec.pdf (Only available in French)

2000 年 8 月 14 日立法實施，該法對於不請自來之商業廣告信息採取「事後拒絕」(Opt-out) 之制度。本法係為實施歐盟先後數個指令而修正盧森堡原有法令所設 (例如，對於遠距銷售之指令或是就指令中對於個人資料之保護規定)，但是，該法並不完全與歐盟 2002/58/EC指令要求之內容相同。

上述法律最新的修正案於 2003 年 2 月 4 日已經提送至盧森堡立法機關[190]，將歐盟 2000/31/EC指令及 2002/58/EC指令具體內容都涵蓋在其中，並將原「事後拒絕」(Opt-out) 之制度變更為「事前同意」(Opt-in) 的制度。

（十一）荷蘭

荷蘭目前尚未有任何特別就有關管制濫發電子郵件立法的法規出現，因此對於荷蘭境內濫發電子郵件造成的問題，只能靠其國內 ISP 業者各自訂定之自律條款以為規範。然而在 2003 年年初開始，荷蘭電子郵件行銷管理協會 (The Email Marketing Management Association of the Netherlands，EMMA-nl) 整合各家 ISP 業者自律條款內之約定，以及荷蘭個人資料保護法及歐盟指令之規定，草擬一部規範濫發電子郵件的法案，推動遊說在歐盟指令規定之期限完成立法。草案中，根據歐盟指令採取了 Opt-in 機制，並對透過 ISP 業者寄發附帶病毒之濫發電子郵件制定處罰規定。然而，國內異議聲浪四起，認為對發送電子郵件加上的諸多限制將會大大縮減網路自由度，而且相關歐盟指令規定需得到收件者直接同意才能對其送發信件的 Opt-in 原則，對於已依契約條款中之約定得到收件者同意對其發送信件的發信人來說，並不公平。隨著歐盟指令規定各會員國實施期限已經屆至，荷蘭的立法動態值得繼續觀察。

（十二）葡萄牙

編號 208/IX/1[a] (PS)之法案具體體現了歐盟 2002/58/EC指令的內容已經在葡萄牙國會審議中。本法案內容可於葡萄牙網站 http://www.cnpd.pt/actos/par/2003/par012-03.htm.下載取得。

[190] See http://www.etat.lu/OLAS/docs/projet5095.pdf (Only available in French)

（十三）西班牙

西班牙對於管理濫發電子郵件之政策採取非常有趣之立法態度。在 2001 年 1 月 18 日所制定的資訊社會及電子商務法（Law on the Information Society and Electronic Commerce）中，立法理由明示大量散發的廣告郵件可增進網路使用之普及率，並有益於資訊社會之發展。但是，事實發展卻是大相逕庭，大眾的猛烈抨擊，使西班牙政府改弦更張，於 2002 年 10 月 12 日實施修正條文，採取「事前同意」（Opt-in）之制度[191]以有效限制濫發電子郵件。

（十四）瑞典

瑞典正針對其於 2000 年 5 月所施行之行銷規範法（*Marketing Practice Act*）進一步依歐盟最新相關指令加以修正。這個法律原先係根據歐盟 97/7/EC 有關遠距買賣之指令訂定，對於利用傳真或是自動撥號系統所發送之廣告信息，採取「事前同意」（Opt-in）原則規範[192]。除此之外，本法規定亦要求任何利用自動系統（即非以使用人工之方式傳送者）傳送訊息的人，應取得收件者之事前同意。瑞典的立法方式頗具彈性，使得該法所得適用之範圍非常廣泛，可以因應通訊方式隨科技之進步變化而適時加以擴張相

[191] Law on the Information Society and Electronic Commerce

Article 21 Prohibitive Rule of Commercial Communications Sent by Email or Other Equivalent Electronic Means of Communication

(1) The distribution of promotional or advertising communications by electronic mail or equivalent electronic means is forbidden if they have not been solicited before or if they have not been explicitly authorized by the recipient.

(2) Commercial communications sent by email or by equivalent means of electronic communication, in accordance with set terms, have to start with the word "*publicidad*" ("publicity").

Article 22 Legal Rights of Recipients of Commercial E-Communications

(1) In case the user of an internet service has to give his email address during the contracting or subscription process with the service provider and the provider has the intention to use this address afterwards for the purpose of sending commercial communications to the customer, he has to inform the customer of this intention. Also he has to ask for the customer's approval to do so before finally concluding the contract procedures.

(2) The recipient has at any time the right to withdraw his given consent to receive commercial communications by simply notifying the sender of his wish to do so.
For this purpose the service provider has to set up easy operating procedures free of charge to enable the recipient to revoke his once given permission. Thus the service provider ahs to make information available regarding those procedures and they must be accessible by electronic means.

[192] **13a** § A supplier may not advertise to a natural person using telefax or an automated dialing system or other similar automatic system for individual communication not operated by a human, unless that natural person has agreed beforehand.
A supplier may use other means for individual communication over distance unless the natural person has clearly objected to the use of that method.

關法律之適用。

（十五）英國

在英國，電子郵件地址通常包含個人之姓名，因此往往被視為個人資料之一部份，對於電子郵件地址的蒐集整理及利用，當然涉及到個人隱私權保護之問題。

英國先在 1998 年，針對實踐歐盟 1995 年個人資料保護指令(European Data Protection Directive 95/46/EC)，制定個人資料保護法(Data Protection Act 1998) ，將所有對自然人個人資料包括且不限於姓名、地址、電話號碼及電子郵件地址之蒐集、處理及利用，全部納入規範。該法保護範圍雖然不及於法人團體，但是對於受僱於法人團體之自然人一樣提供保障：透過事後拒絕(Op-out)機制的建立，所有運用直銷(Direct Marketing)方式的商業組織都必須設有個人資料檔案維護負責人(Data Controller) ，來執行本法所定一切蒐集處理及利用個人資料的規定事項，違反者視其情節輕重，得由主管機關(即 Information Commissioner)對檔案維護負責人處以罰鍰，命令強制其改善；受害的自然人也可以起訴請求賠償損害。儘管如此，英國至今還無適用本法對濫發電子郵件發信人(Spammer)處分的例子。其他違反本法事例所受罰鍰處分最高者為 2002 年對某販賣名單業者處罰 5000 元英鎊。

英國政府為了實施歐盟「電子通訊中個人資料處理及保護個人隱私指令」(Directive 2002/58/EC)，於 2003 年 3 月 27 日起至同年 6 月 19 日舉辦一系列公聽會[193]，並在 2003 年 9 月 18 日由內閣依 1972 年歐洲共同體法授權規定，訂定 2003 有關保護隱私及電子通訊之規定（The Privacy and Electronic Communications(EC Directive) Regulations 2003）[194]，提出於國會同意，自 2003 年 12 月 11 日生效。

上述規定遵守歐盟「電子通訊中個人資料處理及保護個人隱私指令」訂立的框架及原則所定對各種通訊服務自然人用戶之保障，將規範濫發電子郵件以及相類似電子通訊服務(例如傳送文字訊息的呼叫器/手機簡訊即屬之)的主要內容規定在第二十二條及

[193] See http://www.dti.gov.uk/industries/ecommunications (visited on 2003/8/16)

[194] **請參見附件二十三**---英國 2003 保護隱私及電子通訊規則UK Privacy and Electronic Communications (EC Directive) Regulations of 2003

第二十三條[195]。該規定第二十二條第二項規定，非經收件者事前同意，任何人皆不得為直銷目的(for the purposes of direct marketing)傳送，或教唆傳送不請自來的電子郵件給任何自然人用戶(法人團體或其雇員使用法人團體電子郵件信箱者不在此限)，明白揭示原則上採取事前同意(Opt-in)機制。相同的事前同意機制也適用在使用自動撥號系統進行的電話語音及傳真直銷。同條第三項規定例外採取事後拒絕(Opt-out)機制之情形為：

(1) 發信人發送郵件前已經在與該特定收件者就其所提供商品或服務交易或磋商交易過程中取得該特定收件者之聯絡資料；
(2) 該直銷行為是為提供該特定收件者相類似的商品或服務；
(3) 收件者在其個人資料被蒐集建檔的同時，已經被賦予簡易可行的拒絕/ 退出機制，而且未於隨後的通訊中明示反對發信人利用其個人資料對其進行直銷。

任何用戶也不得將其向電信業者申租取得使用權的線路提供與他人從事違反第二十二條規定禁止的行為，該規定第二十三條則禁止發信人在發送的直銷電子郵件中掩飾或捏造其身分識別，也強制發信人必須在發送的電子郵件中提供收件者有效的回覆地址以選擇拒絕再接受郵件。

---

[195] **Use of electronic mail for direct marketing purposes:**
22. - (1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.
(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.
(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where –
(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;
(b) the direct marketing is in respect of that person's similar products and services only; and
(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.
(4) A subscriber shall not permit his line to be used in contravention of paragraph (2).

Use of electronic mail for direct marketing purposes where the identity or address of the sender is concealed
23. A person shall neither transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by means of electronic mail -
(a) where the identity of the person on whose behalf the communication has been sent has been disguised or concealed; or
(b) where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided.

在本規定中，事後拒絕機制也適用於以瀏覽器紀錄程式(Cookies，或稱餅乾檔案程式)蒐集用戶相關網路活動資料及個人資料之情形；所有網站經營者(Marketer)對於其使用瀏覽器紀錄程式蒐集用戶端電腦資料的目的必須有清楚且詳盡的說明，符合有關隱私權保護政策及瀏覽器紀錄資料的規定；並且應提供機會讓用戶可以隨時拒絕網站經營者使用其瀏覽器紀錄資料。英國貿易及工業部（The Department of Trade and Industry）就此建議，網站經營者應提供詳盡說明，來教導用戶如何設定自己電腦上的瀏覽器以避免餅乾檔案程式植入[196]。

2003 保護隱私及電子通訊規定的制定，引發電子商務經營者及直銷業者很大的疑慮。他們認為，新的規定等於是就現行制度做了一百八十度的轉變，各方紛紛提出要求，希望英國隱私權保護主管機關 Information Commission 儘早對上述規則做進一步更明確的解釋。Information Commission 在 2003 年 11 月發佈了 2003 保護隱私及電子通訊規定的指導綱領（the Guidance on Privacy and Electronic Communications 2003），英國法律界普遍的評價是，從這份指導綱領內容看來，Information Commission 事實上是以務實的態度從寬解釋規則的條文，但是仍然謹守著歐盟「電子通訊中個人資料處理及保護個人隱私指令」畫下的界限並未逾越。例如：

- 就所謂磋商交易過程中所獲得特定收間人之個人資料，不以該交易事實上已完成為限，才得以利用。綱領中舉例，在促銷競買活動中所取得參加者資料，即屬於事前同意原則之例外情形。
- 除非收件者表達其不想繼續接收郵件之意願，在 2003 保護隱私及電子通訊規則正式實施前，已經編輯且有適當隱私權保護措施之電子郵件地址名錄資料庫，仍可繼續利用。
- 寄送予公司用戶之電子郵件並不適用本規則之事前同意規範，但是發信人應隨函提供其身分辨識資料及聯絡方式。又在英格蘭、威爾斯以及北愛爾蘭（不包括蘇格蘭在內）境內之無限責任合夥組織，若以其合夥關係單獨成為直銷寄送電子郵件之用戶時，在此合夥關係內之所有合夥人皆受到本規則內對自然人用戶之相同保護，非僅祇單一顯名之合夥人受到保護而已。

[196] See http://www.worldebusinesslawreport.com/index.cfm?selectedpub=1,8&action=dsp_item&id=2328&xprint=1 （visited on 2003/10/29）

- 收件者未拒絕繼續接收直銷目的之商業電子訊息，包括電子郵件、呼叫器/手機簡訊或傳真信件，並不代表收件者已同意繼續接收。
- 若發信人之電子郵件地址名錄為買來或租來的，則發信人須得到名錄上收件者之個別同意，才可寄送郵件。
- 同一家公司以控股型態持有不同事業，或直接持有不同商標，在交易過程中取得的特定收件者資料，除非經各該特定收件者事前同意，不得用於共同業務推廣或資訊交互運用。

該指導綱領以實例問答方式，就本規定之各種適用情形進行釋疑，對於有關電子通訊服務提供者就本規則特定議題在關鍵定義上可能產生的執行上爭議，包括對個人資料之管理與保全瀏覽器紀錄資料程式之使用、網站瀏覽流量資料、用戶帳單資料管理、用戶所在地資訊(Location Data)等，都區分自然人及法人之不同情形，分別有專節依其性質分類詳細敘述。例如，ISP業者是否可保留使用者瀏覽網站時所留下的買賣紀錄、IP位址資料，指導綱領做了相關說明，除非在特定情形，ISP業者需要清算其買賣紀錄來追繳帳款時或事先取得使用者的同意，允許其使用該紀錄時，這些資料才可被拿來利用[197]。

值得一提的是，英國民間各相關產業自訂的自律規範也已經及時參照歐盟隱私保護指令及前述英國 2003 保護隱私及電子通訊的規定，進行修正及補充。以英國廣告行為自律委員會(The Committee of Advertising Practice)為例,該委員會成員包括了英國廣告協會、直銷協會、皇家郵購協會等十九個公協會業者，早前於 2003 年 3 月發布有關廣告、行銷推廣及直銷的規定（British Code of Advertising, Sales Promotion and Direct Marketing）第 11 版，具體規範各公協會成員電視及廣播以外一切廣告及行銷行為，包含報紙、雜誌、郵購宣傳品、活動看板、傳真、呼叫器/手機簡訊以及電子郵件，全部皆在其規範範圍內。隨後，於同年 9 月再更新及擴大前述自律規範：

-應受規範的主體不僅為廣告主（marketer），其他與廣告主市場行銷行為有關聯的人，如廣告代理機構（agencies）或發行人（publishers）等，亦須遵守自律規範規定；
-未經收件者事前同意接收的電子郵件、傳真和手機簡訊廣告都必須清楚於傳遞訊息主旨載明廣告目的，並須揭示發信人全名及

[197] See http://www.linklaters.com/pdfs/practiceareas/ip/Hottopic_ICGuidelines.pdf (visited on 2003/11/25)

聯絡方式；

-廣告主必須隨時確認，其發送的行銷廣告郵件切合其預定目的，且其資料庫裡有關同意收受廣告收件者的資料是最新的；

-以電子郵件、傳真或呼叫器/手機簡訊寄發廣告前，須先得到預定收件者之同意。廣告主寄送相同或類似產品及服務的廣告給其既有客戶，例外地可以不必再重新徵求收件者的同意，但是在每一次發送的訊息中都要明白給予收件者有拒絕再接收的機會[198]。

執行這一部自律規範的是上述業界團體在 1962 年成立的獨立機構-廣告標準自律會（Advertising Standards Authority，ASA），其負責受理及調查消費者對業界成員廣告行銷行為的申訴，具體約束業界成員相關作為都須符合上述同業自律規範。就在 2003 年 12 月初，ASA 就公告其依新規範懲戒的第一個例子:某個廣告主向專門銷售銷售名單的業者買入一份名單，並依這份名單廣寄大量廣告郵件，經消費者申訴，ASA 介入調查，該廣告主辯稱其以為名單銷售業者取得的名單應該都已經事前向名單中所列收件者事先徵得同意。但是，ASA 堅守隱私保護綱領及上述業界自律規範要求，對該廣告主做成書面警告，責令改正，並公開供公眾知悉。

玖、俄羅斯

俄羅斯在對抗濫發電子郵件的議題上，目前是由該國國會設置的國家聯合教育、科學、文化整合資訊計劃（United Nations Educational, Scientific and Cultural Organization Information for All Programme）展開制訂管制濫發電子郵件法案的工作。這個法案是依循目前已存在憲法及 1995 年個人資料保護法有關廣告、個人資料保護及隱私權保護等法律框架設計相關規範。

依目前已知的草案條文，所有違反下列規定散發的商業性電子郵件都在禁止之列，這些規定包括：

一、散發電子郵件給不特定多數人；

[198] See http://www.worldebusinesslawreport.com/index.cfm?selectedpub=1,8&action=dsp_item&id=1886 (visited on 2003/10/15)

二、收件者已明白表示不希望收到來自發信人或第三人委託寄件的來信；

三、發信人經由非法收集電子郵件地址的手段來發送郵件（例如利用蒐集程式從網路上輯錄電子郵件地址）。

草案條文規範了濫發電子郵件發信人，包括個人發信人或受託進行發信工作的公司機構，甚至提供規避郵件過濾器軟體或蒐集電子郵件地址資料的人，違反規定時應負的民事損害賠償責任，以及應納的行政罰鍰。

拾、國際研究比較總結

從上述各國制訂管制濫發電子郵件法規的內容予以綜合分析，我們可以發現，同樣是管制濫發電子郵件問題之法規，各國對於管制的寬嚴程度皆不盡相同，即使是統一依照歐盟指令下之規定來立法的歐盟各國，會員國管制濫發電子郵件法規裡的各個細節仍有不少差異存在。其中最明顯的例子，便是各國在採取 Opt-in 或 Opt-out 機制上的不同。

以歐盟指令的規定內容來看，其立法方式為採取所謂「有彈性的 Opt-in 機制」，亦即其原則上禁止任何人濫發未事先得到當事人同意的電子郵件，然而在發信人因基於之前的商業關係或交流而已握有收件者的電子郵件地址時，即毋須再次得到同意，可以繼續寄發含有相同或類似產品資訊的電子郵件給收件者。此外，歐盟指令也禁止寄發隱藏或偽造發信人身份的郵件，同時亦要求所有的濫發電子郵件皆須在郵件內包含有效的回函地址，供收件者未來不想再接到此類郵件時可以選擇不再續訂。

然而，除此之外，歐盟指令還提供了一個以減少濫發電子郵件問題作為考量的法規中看起來十分不合理的例外，這便是歐盟指令中的 Opt-in 機制只限於寄送郵件給「個人用戶」(Individual subscribers)時才有適用，換句話說，濫發電子郵件給企業用戶之行為並不違反歐盟指令。雖然歐盟執委會委員 Erkki Liikanen 指出，會員國在制定其管制濫發電子郵件內國法時，可以視需要將此規定延伸適用至企業用戶，然其終究不是一個強制會員國履行的規定。

在所有歐盟會員國中，丹麥是最早將歐盟指令中 Opt-in 規定付諸法律的國家，但此後幾乎所有的歐盟會員國皆採取此種機制，作為其管制濫發電子郵件之規定。英國雖遲至 2003 年 9 月才依據歐盟指令制定管制濫發電子郵件的內國法，然而其仍維持 Opt-in 機制不適用於企業間電子商務行為的規定。不過，近日已有英國國會議員團體訴求企業間電子商務行為亦應適用 Opt-in 機制的聲音出現。

澳洲管制濫發電子郵件法規也採行 Opt-in 機制，只是其規範內容和歐盟指令大不相同。其最大不同之處，在於歐盟指令允許發信人基於先前的商業關係或交流而已握有收件者的電子郵件地址時，毋須再次經過其同意，可繼續寄發含有相同或類似產品資訊的電子郵件給收件者，而澳洲的法律並不特別強調須基於先前的商業關係或其他交流，而只是單純的禁止未得到收件者的事前同意便不能寄發信件。但如此含糊不清的規定，也許會引發更多後續的問題。此外，澳洲的管制濫發電子郵件法案也明文將所有來自政府、政治、宗教、慈善及教育團體等的大量電子郵件排除在法規規範之外，其例外之範圍顯然較歐盟指令來得廣泛許多。

另一方面，美國政府仍不情願將 Opt-in 機制納入其法規規定中。從目前仍在美國議院中審查的各項管制濫發電子郵件法案及已通過的 CAN-SPAM ACT 來看，仍以採行 Opt-out 機制為主流。這些法案，皆允許無限制發送電子郵件，直到收件者拒絕繼續收受郵件為止。其中，尚未通過且採取 Opt-out 機制的法案，包括了 2003 反濫發電子郵件法案（Anti-Spam Act of 2003）、降低濫發電子郵件散佈法案（Reduction in Distribution of Spam Act）、減少濫發電子郵件法案（Reduce Spam Act）。

除了採取 Opt-out 機制這個特點外，美國反濫發電子郵件法案亦規定這些電子郵件須在其主旨欄上標示出廣告的字樣，並禁止其使用錯誤或使人受到誤導的標題作為主旨，有些法案亦嚴格禁止利用自動獲取或蒐集電子郵件地址的軟體程式。其中，在已經完成立法的 CAN-SPAM ACT 還包括另一項有趣的特色，按照該法案規定，在其通過後，美國聯邦貿易委員會必須設計提供一份「不要濫發電子郵件」名單（Do-Not-Email list），讓那些不想收到濫發電子郵件的人可以上去登記，而濫發電子郵件者從此不得再寄送電子郵件給這些人。這項規定引來許多批評，而這些批評多半基於下列兩點：第一，濫發電子郵件者反而有確切的電子郵件地址可以對之散佈寄送；第二，即使 CAN-SPAM ACT 生效施行，聯邦貿易委員會

也不可能會真的去執行提供製作這張表單，而這項法律最終也只是個單純採行 Opt-out 機制的例子而已。同樣採取 Opt-out 機制，且規定須在信件主旨上標示廣告字樣的國家，還有日本以及韓國。

在上述採取制定法規作為管制濫發電子郵件手段的國家外，還有一些國家採取其他方法對抗濫發電子郵件。例如，加拿大雖然制定了一部規範電子商務市場的法律，但該法對於處理濫發電子郵件的規定卻是非常寬鬆；新加坡則是試圖透過業者自律，鼓勵網路服務業者訂定並執行其對抗濫發電子郵件的政策；紐西蘭則已選擇藉由科技發展及教育公眾等手段作為其對抗濫發電子郵件問題之策略。

由此看來，並沒有一部真正完美的法律可以完全解決濫發電子郵件問題，特別是在面對網際網路行為的管轄權及執行力議題上。然而可以確定的一點是，光靠業者自律，並不足以管制濫發電子郵件的蔓延，而單靠科技進步或是培養公眾自覺意識，同樣無法達到目的。想要徹底解決濫發電子郵件問題，最終還是必須靠著上述幾種方法齊頭並進，多管齊下，並確實實施及執行管制濫發電子郵件法規，才能有效降低濫發電子郵件的數量。

觀察各國制定管制濫發電子郵件之法規，或是其他相關辦法來對抗濫發電子郵件問題，可以歸納出下列結論：

一、立法規範濫發電子郵件問題已經成為國際趨勢：

美國自從各州相繼自 1997 年開始制訂法律規範濫發電子郵件問題之後，到目前為止，已有三十六州對濫發電子郵件問題立法規範，而聯邦也已通過管制濫發電子郵件的 CAN-SPAM ACT。

另外，歐盟會員國、日本、韓國，也已針對濫發電子郵件問題予已立法規範；甚至在中國大陸、新加坡、俄羅斯等尚未立法規範之國家，也已開始準備立法中，由此可見對於濫發電子郵件之問題，制定立法規範予已管制，已經成為國際趨勢。

二、Opt-in 與 Opt-out 之適用選擇：

對於讓網路使用者不接收濫發電子郵件的機制，已立法規範濫發電子郵件的國家究竟應採 Opt-in 或 Opt-out 機制為妥，一向見仁見智，端看各國國情及經濟變化狀況如何影響。依照目前歐

洲各國立法情況來看，Opt-in 機制仍是歐盟會員國主要採行的機制，少數國家如愛爾蘭、盧森堡等國，也為了順應歐盟指令規定而作出調整，從原本的 Opt-out 機制改為 Opt-in 機制；而美國、日本及韓國則選擇以 Opt-out 機制為主。

在國際合作方面，來自歐盟的壓力頻頻催促美國採行 Opt-in 機制，通過更嚴格的管制濫發電子郵件法律。因此，雖然美國日前通過的 CAN-SPAM ACT 仍未採行 Opt-in 機制，但在未來對於消費者隱私權保護意識更為高漲的情況下，Opt-in 機制是否會逐漸取代 opt-out 機制，仍值得持續觀察注意。

三、不請自來的傳真、簡訊及電話亦納入規範：

美國聯邦貿易委員會原本預定於 2003 年 10 月 1 日上路施行之電話勿擾法案（Do-not-call），在丹佛上訴法院遲遲未對電話行銷業者所提之違反言論自由的上訴作出判決的情況下，只得暫緩執行此一措施，然而此法在美國所引起的迴響，充分顯示出在目前新興科技不斷被用來作為新的行銷手段之時，消費者對這類不請自來的訊息，無論是電子郵件，抑是其他如傳真、手機簡訊等等訊息，已經感到不勝其擾了。

從上述各國最新法制發展情形中，我們可以看到，歐洲各國因為歐盟指令之規定，大部分國家已經將利用自動電話系統撥打不請自來的電話納入規範中，規定電話撥打者應於打電話之前取得受話者之同意，甚至在奧地利、丹麥、瑞典及比利時等國家，已將其規範範圍擴張到對於任何利用自動系統傳送之廣告訊息，皆須受到這些法規的規範，無論這些訊息是以電子郵件、傳真、手機簡訊或電話等形式出現。

另外，日本由於無線通訊發展快速之關係，其居民通常以行動電話收取電子郵件，且觀看這些電子郵件亦須另外付費，導致其手機廣告簡訊氾濫問題成為最大困擾，因此在其特定電子郵件法及特定商業交易法之相關規定中，不僅規範以電腦收發的信件，還包括以行動電話收發的廣告電子郵件。因此，在利用新興科技作為行銷手法越來越盛行的情況下，將不請自來的傳真、電話、手機簡訊等訊息一同予以規範，將會成為未來的立法規範發展趨勢。

四、國際合作是反制濫發電子郵件之下一步驟：

在越來越多國家訂立管制濫發電子郵件法規之時，我們不免也將面對另一隨之而來的問題：網路無國界及其無遠弗屆的特性正是其魅力所在，因此即使在本國訂立管制濫發電子郵件之法律，濫發電子郵件者仍可轉移陣地至那些未對濫發電子郵件問題立法管制的國家發信，以規避法律規範，如此一來，是否即意味著，光靠立法並不足以應付濫發電子郵件的問題？我們是否需要其他更全面、更有力的行動來解決這個跨國性的棘手問題呢？

目前國際各國主政機關已意識到這個潛在問題，並試圖透過國際合作來予以解決。在這方面進行得最成功的區域，首推歐盟。由於歐盟 2002/58/EC 指令命令各會員國須於 2003 年 10 月底前完成管制濫發電子郵件問題的立法工作，整個歐盟會員國內國市場將有一個具有統一標準的法律規範出現，使得歐盟各國在對付濫發電子郵件的問題下達到一致的目標，同時也能相當程度地減少濫發電子郵件者逃至他國發信以規避法律的情況發生。

美國目前已有超過三十州訂立州法以管制濫發電子郵件問題，然而美國至今仍是世界上最大的濫發電子郵件來源國。這種情況除了顯示出美國在執行其相關法律的成效上存有疑問之外，歐洲幾個立法較為嚴格的國家，例如英國，也對美國管制濫發電子郵件的情形表示不滿，認為美國是因為其國內州法對電子郵件的規範較為寬鬆，才會導致這種情況發生，因此，英國甚至有國會議員在 2003 年 10 月間組成遊說團體對美國進行遊說，企圖說服美國通過更嚴格的聯邦管制濫發電子郵件法案以為解決。

除了先進國家間就濫發電子郵件法案進行統一標準及互助合作的行動外，尚未制定管制濫發電子郵件相關立法的國家更是有可能變成濫發電子郵件者滋生的溫床及避難地。面對此種難題，前往美國進行遊說工作的英國國會議員Brain White 也表示，各國除了立法管制國內濫發電子郵件問題外，打破疆界藩籬，尋求國際合作，共同打擊濫發電子郵件者，才是徹底解決問題正本清源之道[199]。

[199] **請參見附件五---**訪問英國國會議員Mr. Brian White, MP（Member of Parliament in the United Kingdom and Treasurer of the All Party Parliamentary Internet Group）針對濫發電子郵件問題之訪談紀錄 2003/11/06.

表 3.3　世界各國管制濫發電子郵件法令比較

國家	立法進度	法令名稱	收件者名單保留機制	刑事處罰
美國	已有 36 州州法規範及聯邦立法	⦿CAN-SPAM ACT	Opt-out	有
日本	於 2002 年通過新法，且修正舊法規範	⦿特定商業交易法修正 ⦿特定電子郵件法	Opt-out	有
韓國	於2001年立法通過且生效	⦿ Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 (促進資訊、通訊、網路利用及資訊保護法)	Opt-out	有
新加坡	無	無	無	無
中國大陸	無	無	無	無
澳洲	2003 年 11 月通過立法	⦿A Bill for an Act about Spam, and for Related Purposes (Spam Bill 2003)	Opt-in	有
歐盟	2002 年 7 月通過相關新指令	⦿Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communica- tions Sector (Directive on Electronic Communications) 歐盟 2002/58/EC 電子通訊下之個人資料處理及隱私權保護指令)	Opt-in	無
奧地利	已依歐盟指令 2002/58/EC 完成修法	⦿the Telecommunication Act(電信法)	Opt-in	有
比利時	2003 年 3 月立法通過且生效	⦿the Law on Certain Legal Aspects of Information Society Service (資訊社會服務相關法律)	Opt-in	無
丹麥	2000 年 7 月立法通過且生效	⦿Marketing Practices Act (行銷規範法)	Opt-in	有

芬蘭	1999 年修正舊法之規範	⦿Data Security Act (資料安全保護法)	Opt-in	無
法國	2003 年 2 月提出新法法案,目前等待國會審議中	待查	Opt-in	無
德國	預計將於2003年底完成制定相關法案規範	待查	Opt-in	無
希臘	國會審議相關立法中	待查	Opt-in	無
愛爾蘭	已通過最新法令修正	⦿European Communities Regulations 2003 (2003/12/20 加入歐盟應配合履行的有關規定)	Opt-in	無
義大利	新法於 2003 年 9 月 1 日生效實施	DL975/1996 DL171/1998 DL185/1999	Opt-in	有
盧森堡	2000 年 8 月立法通過且生效	⦿Law Related to Electronic Commerce (電子商務法)	Opt-out	無
荷蘭	目前正在研擬草案	待查	Opt-out	
葡萄牙	新法案已提交國會審議	⦿208/IX/1ª (PS)	Opt-in	無
西班牙	2002 年 10 月制定新法	⦿Law on the Information Society and Electronic Commerce (資訊社會及電子商務法)	Opt-in	無
瑞典	增訂修正規範中	⦿Marketing Practice Act (行銷規範法)	Opt-in	無
英國	2003 年 12 月 11 日新法生效	⦿Privacy and Electronic Communications (EC Directive)Regulations 2003 有關隱私及電子通訊之規定)	Opt-in	無
俄羅斯	正擬議制定新法規範中	無	Opt-in	無

第四章　我國管制濫發電子郵件行為相關規範之檢討

壹、濫發電子郵件對網路使用造成的影響

根據交通部 2003 年 12 月發布統計資料顯示，截至 2003 年 6 月底為止，我國網際網路使用人數達到 876 萬人，上網普及率為 39%，平均 2.6 人就有一人使用網路，在亞洲地區排名第五，次於韓國、新加坡、日本及香港。但是，在寬頻普及率的表現上，依據國際電信聯合會(ITU)統計排名，至 2002 年 12 月止，我國寬頻上網普及率為 9.4%，居全球第四，僅次於韓國(21%)、香港(14.9%)及加拿大(11.2%)。

經濟部技術處委託資策會，進行 2003 年我國企業網路應用調查結果顯示，2003 年台灣整體企業連網率(泛指企業所進行的任何網際網路運用包括電子郵件企業網站建置及電子商務應用等)達 79%，相較於 2002 年同期，增加了 17%，這些增加的成長比例主要來自於中小企業家數的大幅增加。其中，使用電子郵件的比例，由 2002 年的 52%成長至 2003 年的 74%，顯見企業日常營運依賴電子郵件服務之程度極深。

在我國對外連網頻寬發展方面，依資策會及台灣網路資訊中心(TWNIC) 所做台灣網際網路連線頻寬調查結果顯示，到 2002 年 12 月為止，我國國外連線頻寬達 14,790Mbps，相較 2001 年同期，成長一倍。其中，美國、日本、香港、中國大陸、新加坡以及韓國，依序為我國對外頻寬連網主要國家及地區[200]。

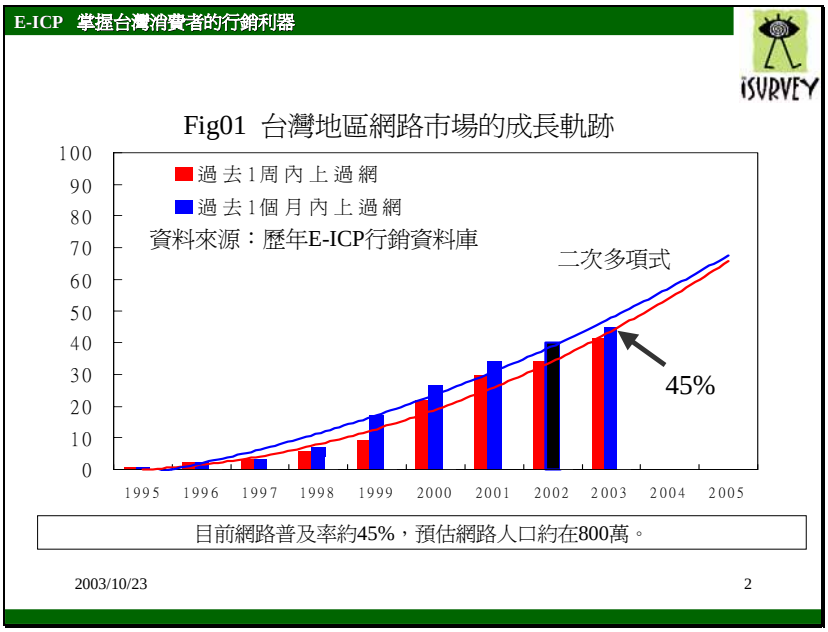
根據前述資料顯示，目前台灣的網路使用者數目以每年增加將近一百萬人的速度成長，然而對於濫發電子郵件行為感到困擾的比率，也由 2002 年僅佔所有網路使用人口的 7.4%，攀升到 2003 年的 11.8%，其成長幅度高達 59%[201]。根據市場研究公司估計，網路使用者對網路上濫發電子郵件氾濫感到困擾的比例，在 2004 年可能更高達 50%以上。另外，在網路使用行為的主要困擾上，2003 年的實證調查數字顯示，也有高達 26.5%的上網人口對垃圾資訊太多感

[200] 詳見經濟部技術處，＜2002 網際網路應用及發展年鑑＞，2002 年，頁 33 以下

[201] 見附圖 4.2，資料提供：東方線上www.isurvey.com.tw

到不滿[202]，顯示在台灣網路使用越來越普及的情況下，濫發電子郵件行為造成的影響程度，正在逐步升高。台北市消費者電子商務協會所做一項尚未經證實的調查估計則透露，我國每年得花費新台幣六百億元以上的社會成本來處理濫發電子郵件。

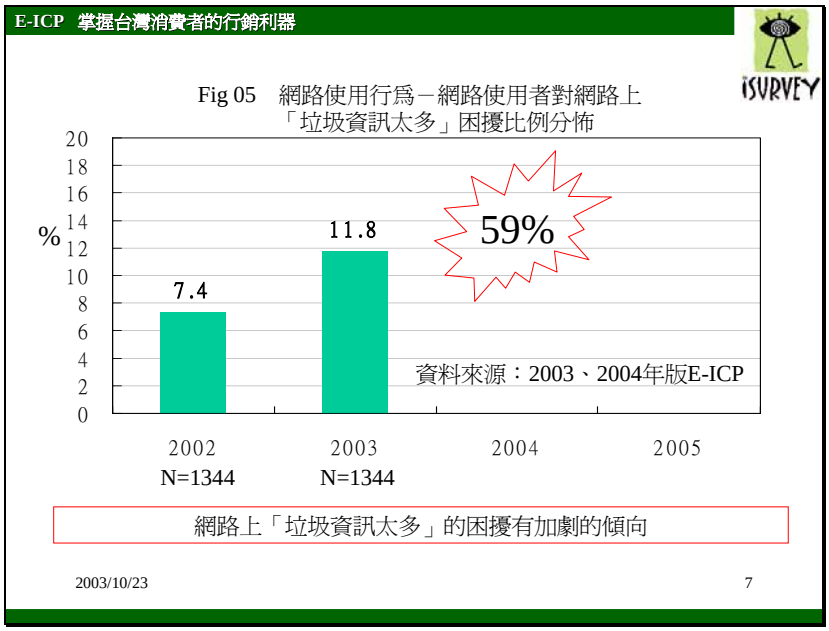
【圖 4.1 台灣地區網路市場的成長軌跡[203]】



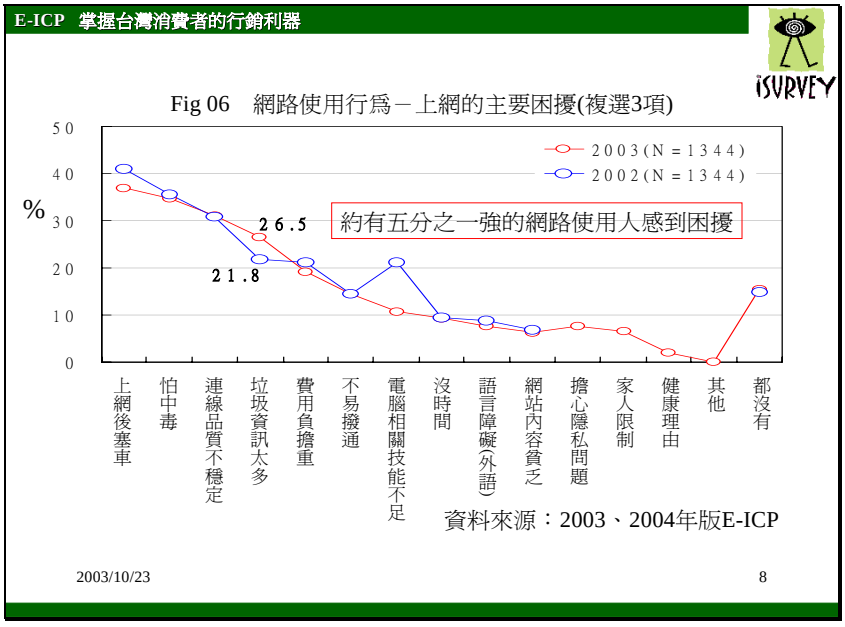
[202] 見附圖 4.3，資料提供：東方線上www.isurvey.com.tw

[203] 資料提供：東方線上www.isurvey.com.tw

【圖 4.2 網路使用行為－網路使用者對網路上「垃圾資訊太多」困擾比例分布[204]】



【圖 4.3 網路使用行為－上網的主要困擾[205]】



204 資料提供：東方線上www.isurvey.com.tw

205 資料提供：東方線上www.isurvey.com.tw

台灣終止童妓協會在 2003 年 10 月委託蕃薯藤入口網站，進行網路調查發現，78%網路使用人每週都會收到色情訊息；而發生在鄰國日本及韓國濫發手機簡訊影響使用人權益的情形，在我國也日益嚴重。交通部電信總局 2003 年 12 月發布資料顯示，我國每年約有二億通的簡訊使用量，其中有約 10%，即二千萬通為詐財內容之簡訊。綜合上述網際網路使用者與行動電話使用者面臨濫發電子訊息威脅之處境，濫發電子郵件不僅已造成使用者之困擾，其背後所隱含對於隱私權的侵害更不容小覷。

在 ISP 業者關心的項目上，濫發電子郵件之大量傳送行為及其內容不僅包含詐財及色情，甚至具有電腦病毒，危害網路傳輸安全，更成為我國發展電子商務產業之隱憂。本研究對我國 ISP 業者進行訪談調查結果也顯示，ISP 業者普遍已經不相信，可以單獨依賴用戶服務契約約定來遏止或減少日益增加的濫發電子郵件。尤其嚴重的是，濫發電子郵件猖獗的狀況不加緩解，已使得與我國連網的外國及地區 ISP 業者針對我國 ISP 業者連外電子郵件發送採取攔堵及封鎖措施。

2003 年 9 月，中國的互聯網協會公佈，將我國多數主要 ISP 業者伺服器位址列入反濫發電子郵件黑名單，並開始執行拒絕接入動作，造成各該 ISP 業者用戶連外電子郵件無法送入中國地區。稍早之前，中華電信也曾遭遇美國 AOL 等 ISP 業者對來自我國伺服器傳送電子郵件攔堵之情形。

本研究以電子郵件對外國受訪對象進行採訪期間，也屢次遭遇送出的電子郵件頻頻被退回的窘況。經過深入了解發現，多達數百個美歐國家企業網站及 ISP 業者在網頁上明示，其網站拒絕接收來自中國、台灣、韓國、巴西、阿根廷等國家 IP 位址之電子郵件。濫發電子郵件造成的影響，已經不僅是內國公安秩序之問題，更已削弱了我國企業及民眾實際利用網際網路進行國際聯絡的能力與尊嚴地位。

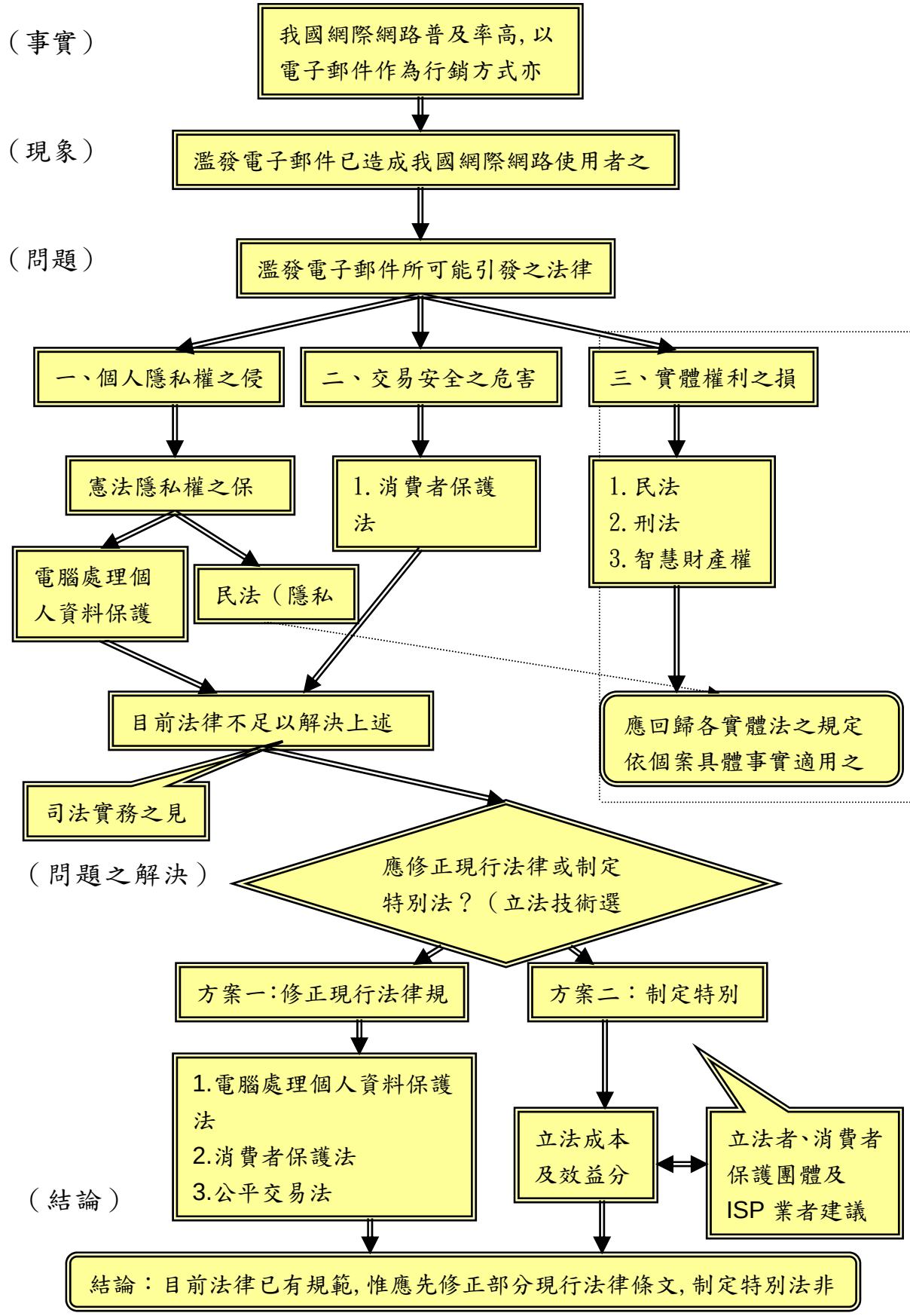
貳、濫發電子郵件涉及之相關法律問題

本研究進行國內外訪談相關立法者、執法者及實務界、學術界人士，關於濫發電子郵件現象衍生之問題，眾多受訪者異口同聲表示，濫發電子郵件引發的問題，不止一個，而且錯綜

複雜，因此所需考量的解決方案也不會只有一端。本研究整理我國 ISP 業者所提供濫發電子郵件行為態樣，並分別深入以現行各項可能援引以管制濫發電子郵件現象及行為之法律，檢討其適用關係，依其危害法益之種類，區分出三個面向，即濫發電子郵件對於個人隱私權之侵害，對於交易安全之危害以及對於其他實體權利之損害，同時在本節進行討論。

在進一步應該採取的立法作為或修法動作方面，則根據對既有法律體系因應濫發電子郵件現象已見的漏洞與不足之處，參酌前述國際研究當中發現之各國不同做法，思考管制手段之選擇。圖 4.4 列示本研究所整理我國關於管制濫發電子郵件之法制思考流程。本研究以為，關於法律上之解決方式，宜考量我國之產業環境及現行法制現狀。目前我國在關於個人隱私權、交易安全及財產權保障方面，已有相當健全之法制體系，因此在討論增置必要的管制手段前，應回頭檢視目前法制是否有闕漏不足或窒礙難行之處，並整體檢討立法成本及效益分析。

【圖 4.4 我國關於濫發電子郵件之法制思考流程圖】



本研究調查歸納，濫發電子郵件行為在我國之態樣，至少包括如下情形:

(1)未經同意，擅自蒐集網路使用者電子郵件地址及其他個人資料加以利用(E-mail Addresses Harvesting)；

(2)虛偽標示郵件來源，以掩飾及混淆收件者對於濫發電子郵件真正來源的認知(Brand Spoofing)；

(3)侵入他人電腦，以電腦程式干擾，使利用為發送大量電子郵件之工具(Hijacked Relays)；

(4)發送郵件內容含有色情(少年及兒童不宜)及不實欺騙的商業廣告(Sexual and Fraudulent Messages)。

濫發電子郵件行為在我國現行法律體系內涉及之相關法律問題，包括對個人隱私權之侵害、對於網際網路交易安全之危害以及對於實體權利包括財產權及個人法益之損害，茲分述如下：

一、對於個人隱私權之侵害

濫發電子郵件涉及之法律問題，主要在於對於個人隱私權之侵害，應分別從憲法及法律層次逐一探討，茲分述如下：

【表 4.1 濫發電子郵件侵害個人隱私權涉及之法律問題】

濫發電子郵件涉及之基本權	憲法位階規定	法律位階規定	相關規定
（個人資訊）隱私權	無明確規定（但大法官會議釋字第二九三號解釋有述及）	電腦處理個人資料保護法	「個人資料」之定義
			適用之範圍
			維護個人資料之義務
			販賣個人資料之處罰規定
		民法	人格權之侵害

（一）憲法關於隱私權之保障

1.隱私權之意義

對於濫發電子郵件之管制在憲法層次上之考量，主要在

於個人不願受到打擾及希望個人資料不被公開揭露之「隱私權」之侵害。

對於隱私權最簡要的定義就是「不受他人干擾之權利」（the right to be let alone）。不受干擾之範圍包括涉及個人屬性、資料、活動及一切與公益無關的私人事務，以及個人對於屬於自身的生活型態及內容所擁有的自我決定權。[206]

1960 年 Prosser 教授在其著名之論文「Privacy」中，對相關案例從事類型分析，歸納出下列四種不同對於隱私之侵權行為，並納入其所編之美國侵權行為法整編（Restatement of Torts, Second），而成為通說：

A. 侵擾原告的獨居、獨自性或私人事務；
B. 公開揭露使原告難堪的私人事務；
C. 公開某事故，致原告遭公眾誤解；
D. 被告為自己利益，未經原告同意，而使用原告的姓名或特徵。[207]

然而，隱私權在近年來已被賦予更具積極性之意義。根據美國賓州大學法學院 Anita Allen 教授的分析，將隱私權依其內容歸納為下列四類：

A. 資訊隱私權（information privacy）：一般人所了解或主張的隱私權，絕大部分是指資訊隱私權。也就是一個人可以自行決定何時、以怎樣的方式，將那些有關個人的資訊公開給誰的權利；

B. 身體隱私權（physical privacy）：指一個人有排除他人接近個人身體或侵入個人生活空間的權利；

C. 自主決定隱私權（decisional privacy）：指一個人有不受政府或第三人干涉個人抉擇的權利；

D. 具財產價值之隱私權（proprietary privacy）：即個人對於隱私權中人格權利益的經濟利用及所有權。[208]

---

[206] 王郁琦、陳炳全，前揭文，頁 155

[207] 王澤鑑，＜侵權行為法第一冊－基本理論一般侵權行為＞，台北市：自版，初版，1998 年，頁 147

[208] 林子儀，＜基因資訊與基因隱私權＞，載於＜當代公法新論（中）＞，元照，2002 年，頁 700 以下

2.資訊自決權之意義

上述關於資訊隱私權之保障，在德國發展之憲法基本權譜系及基本權清單中，又涵攝出所謂「資訊自決權」(Grundrecht der informationelles Selbstbestimmungsrecht)，指每個人基本上有權自行決定，是否將其個人資料（Daten）交付與供他人利用。易言之，個人資料非經本人許諾，不得任意蒐集、儲存、運用、傳遞，若基於公益的理由，必須限制該項權利，當然需遵循民主法治國之諸多原則。[209]

按資訊自決之用語，係經德國聯邦憲法法院 1983 年之「人口普查判決」(Volkszahlungs Urteil）正式提出，且將之列屬一般人格權。[210]依德國「聯邦個人資料保護法」(BDSG）第三條對個人資料所下之立法定義為：「涉及特定或可得特定自然人之所有屬人或屬事之個別資料。」

在今日邁入「知識經濟」的時代中，資訊的及時取得已成為提昇國家競爭力的嚴肅課題，而電訊科技與其事業更成為發展知識經濟產業不可或缺的基礎與平台。其中資訊產業係當代國際「資訊社會」(Informations gesellschaft）概念下蓬勃發展之一個特殊經濟領域，且功能健全之資訊設施與服務係實現人民「個人資訊自決基本權」之基礎，並基於其「基礎設施」(Infrastruktur）之特質對於國計民生的保障具有不容忽視之關鍵性地位。[211]就此而論，濫發電子郵件現象之擴大蔓延，實已妨礙個人關於有權選擇個人資訊是否公開及是否接取資訊之基本權，而有礙行使「個人資訊自決基本權」。

另一方面，自從進入「資訊社會」時代，電腦科技被政府和私人企業普遍應用於蒐集與處理個人資料方面以來，有關個人隱私權如何能受到妥適保護的問題，逐漸成為一個

[209] 李震山，＜論資訊自決權＞，載於＜現代國家與憲法＞，月旦，1997 年，頁 710

[210] 該判決主文略謂：「在現代資料處理之條件下，應保護每個人之個人資料，免遭無限制之蒐集、儲存、運用、傳遞，此係屬基本法第二條第一項（一般人格權）及基本法第一條第一項（人性尊嚴）保護範圍。該基本人權保障每個人，原則上有權自行決定其個人資料之交付與使用。」參見李震山，前揭文，頁 714

[211] 蔡步青，＜我國電信管制革新下頻譜政策之檢討－以第三代行動通訊業務為中心＞，台大國家發展研究所碩士論文，2003 年，頁 2

備受關注的新興法律領域。尤其是在網際網路普及之後，雖然一般人的資訊取得能力因而大增，可是相對的，透過各種網路相關科技的運用，對於網路使用者各種個人資料的蒐集、歸類、重組與分析等等處理，更趨細密與複雜，諸如此類因為各種交易行為而產生的的資料，鉅細靡遺，不僅有如記載個人行蹤的「電子腳印」（electronic footprint），範圍更是廣及個人所到訪的網站、消費習慣、閱讀習慣、甚至信用紀錄、通訊紀錄等，不一而足。而這些個人資料往往被蒐集者進一步轉售給經營直效行銷業務（direct marketing）的個人或組織，作為鎖定（targeting）消費者、以從事其銷售行為的依據。因此，這種個人資料除了表彰個人之特性外，事實上還具有一定之經濟價值。

安・布蘭斯康（Anne Branscomb）在其所著的「出賣資訊」（Who Owns Information: From Privacy to Public Access）一書中提到「我們的姓名、地址與個人交易紀錄，都是有用的資訊財產，我們必須認知到，我們對這些都是有財產權的。」

事實上，也就是對個人資料有「收益」之期待，資訊時代隱私權不再僅具有消極防禦性質，而是在於明白告知及參與決定的個人資料支配權，也就是當事人應有權控制其個人資料之使用。[212]

3.我國憲法關於隱私權之保障

隱私的觀念在我國歷史及文化上並非原生，事實上在近代我國成立民主立憲政體後之國民意識當中，亦並未生根，因此，並無具體事例可資參照為隱私保障之蛛絲馬跡。

綜觀我國憲法本文及增修條文規定，並未明文述及保障隱私權，隱私權是否為憲法保障的一種基本權利，其具體內涵或類型究竟是什麼？隱私能否如上述外國學者分析，在資本主義知識經濟的觀念中，被理解為一種新的財產權，在我國法學界尚無定論。司法院大法官會議在 1992 年做成之釋字第二九三號解釋，首次，也是唯

[212] 簡榮宗，＜網路上資訊隱私權保障問題之研究＞，東吳大學法研所碩士論文，200 年，頁 73

一的一次，言及並正面肯定維護人民之「隱私權」。[213]論者有認為本號解釋雖承認隱私權，但並不認為其為憲法所保障之一種基本權利。不過，王澤鑑大法官則認為本號解釋的重要意義之一，即是「肯定隱私權是憲法上的權利，屬憲法第二十二條人民之其他自由及權利，應受憲法之保障。」[214]

（二）法律關於隱私權之保障

濫發電子廣告郵件之行為涉及個人資訊使用及取得之隱私權保障，已如前述。1999 年 4 月 21 日修正公布民法第一百九十五條，在得請求非財產上損害賠償之人格權侵害類型中，已新增「隱私」類型；而保障隱私權之一般性規定者，則見於 1995 年制定之電腦處理個人資料保護法，茲分述如下：

1.民法關於侵權行為之規定

按隱私權乃不受他人任意干擾之權利，至於電子郵件地址，是否為個人隱私的一部分，則應先檢視該電子郵件地址是否為個人使用其次判斷得否藉由該電子郵件地址直接或間接識別出該特定個人，通常如網路使用者以自己姓名冠於電子郵件地址之前之情形則可以認為該電子郵件地址屬於個人資料而應屬隱私之範圍，受侵害之人，得據民法第一百八十四條第一項前段之規定，請求隱私權受侵害之損害賠償，如所受之不法侵害非為財產上的損害，另得依民法第一百九十五條第一項請求非財產上的損害賠償。

依民法第一百九十五條第一項規定，不法侵害他人之隱私而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。濫發電子郵件發信人雖無侵犯他人隱私或將他人隱私公開之意圖，而僅是藉由蒐集到的電子郵件地址名單大量寄發，此種未經收件者許可之發送行為是否已危害個人對於屬於自身的生活型態及內容所擁有的自我決定權，涉及國情不同，與國民文化上對於隱私認知程度差異，容或有爭議。但是，濫發電子郵件內容往往為色情或詐財欺騙，對於收件者在不知情情形下閱讀，難謂非精神上之騷擾，而收件者正

213 釋字第二九三號解釋略謂：「銀行法第四十八條第二項規定『銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密』，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。」

214 林子儀，前揭文，頁 698

常利用其電子郵件地址進行憲法保障通訊自由的溝通，又受到需逐一耗費時間過濾刪除濫發電子郵件之干擾，此際應認有上述民法第一百九十五條第一項規定之適用。

2.電腦處理個人資料保護法

電腦處理個人資料保護法第一條規定，為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法；而關於個人資料之意義，依同法第三條第一款之定義，係指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。電子郵件地址依使用人是否為自然人，以及是否使用個人姓名或相關表徵，也可以成為本法保護之個人資料，已如前述。

依電腦處理個人資料保護法第三條第七款及第十八條之規定，公務機關、醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業、徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人，對個人資料之蒐集與電腦處理，應有特定目的，並符合法令執掌內、經當事人同意，或原有契約關係存在、已公開之資料、為學術研究而無害於當事人等要件；另外，個人資料利用時，除非符合該法例外之情形，否則基本上必須於蒐集之特定之目的必要範圍內，方可利用其蒐集來的個人資料。[215]

有關個人資料之利用，按電腦處理個人資料保護法第十八條第一款及第二十三條第四款之規定，也需經當事人書面同意，始得為之。[216]因此，意圖營利，違反前開規定而蒐集利用

[215] 電腦處理個人資料保護法第三條第七款規定：「非公務機關：指前款以外之左列事業、團體或個人：
(一) 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。
(二) 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。
(三) 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人」
第七條規定：「公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得為之：
一　於法令規定職掌必要範圍內者。
二　經當事人書面同意者。
三　對當事人權益無侵害之虞者。」

[216] 電腦處理個人資料保護法第二十三條規定：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有左列情形之一者，得為特定目的外之利用：
一　為增進公共利益者。

或販售屬於個人資料之電子郵件地址，依同法第三十三條之規定，可處二年以下有期徒刑、拘役或科或併科新臺幣四萬元以下罰金。[217]

針對本報告主題，有研究論文指出，目前本法並無法從源頭解決濫發電子郵件問題，其一，電子郵件地址單獨存在是否構成本法所稱「足資識別個人身分」之保護客體仍有爭議；其二，規範主體限於八大行業與「以蒐集或電腦處理個人資料為主要業務」者，並無法規範此範圍以外蒐集、利用個人資料者，例如，透過電子郵件地址搜尋軟體在BBS站等討論區搜尋上網者，多非屬「以此為主要業務者」之個人、團體或電子商家，而無法以本法規範，[218]因此，建議將ISP業者列入前揭八大行業。

本研究蒐集與此有關之司法實務見解發現，台灣新竹地方法院檢察署曾於 1998 年，針對有關電腦處理個人資料保護法之適用於濫發電子郵件行為，作成八十七年偵字第五七二三號不起訴處分書，其案例事實略謂：中華電信公司對其某用戶在網路上濫發電子郵件給其他用戶之行為，以違反電腦處理個人資料保護法第三十三條之規定提出刑事告訴，該用戶主要係涉及代客發送電子郵件。承辦檢察官做出不起訴處分，理由是被告濫發電子郵件的行為，雖足致網路使用者之困擾，然而，並未涉及對個人資料之蒐集，且他人人格權亦未因此遭受侵害。[219]

就前述法律實務見解觀之，目前依據電腦處理個人資料保護法反制濫發電子郵件，在解釋上有兩點必須突破，一係濫發電子郵件是否涉及對個人資料之蒐集及利用？一般而言，商家寄發電子廣告信件，通常是藉由發信廣告業者代客發送，或購買來路不明之電子郵件信箱名單後以發信軟體發送，似無涉對個人資料之蒐集，也無揭露他人隱私而造成他人非財產上之損害；至於未經許可之發送行為，是否危害收件者個人對於屬於自身的生活型態及內容所擁有的自我決定權，而侵害他人之人

二　為免除當事人之生命、身體、自由或財產上之急迫危險者。
三　為防止他人權益之重大危害而有必要者。
四　當事人書面同意者。」

[217] 電腦處理個人資料保護法第三十三條規定：「意圖營利違反第七條、第八條、第十八條、第十九條第一項、第二項、第二十三條之規定或依第二十四條所發布之限制命令，致生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣四萬元以下罰金。」

[218] 余德正，＜不法使用網際網路之刑事責任＞，東海大學法研所碩士論文，2000 年，頁 137

[219] 王郁琦、陳炳全，前揭文，頁 163

格權，或僅是一般人可以在合理範圍內容忍之不便利行為或騷擾，恐怕有賴立法者來決定，而非由法律規定本身可以推敲而得。

二、對於交易安全之危害

濫發電子郵件行為危害交易安全涉及相關法律之適用，在個人權益之保障方面，主要有消費者保護法之適用；在事業或企業經營者之保障方面，則依公平交易法之規定及實務見解分析，茲分述如下：

【表 4.2 濫發電子郵件危害交易安全涉及之相關法律】

濫發電子郵件問題涉及之法律	相關規定
消費者保護法	適用郵購買賣之規定
	揭示義務之規定
公平交易法	不公平競爭
	虛偽或錯誤之表示
	其他不正行為之禁止

（一）消費者保護法

消費者保護法第二條第十款規定，所謂郵購買賣係指企業經營者以廣播、電視、電話、傳真、型錄、報紙、雜誌、網際網路、傳單或其他類似之方法，使消費者未能檢視商品而與企業經營者所為之買賣。因此，利用網際網路，使消費者未能檢視商品而與企業經營者所為之交易，也屬於本法規定之郵購買賣，應適用相關的強制規定。

消費者保護法第十八條規定：「企業經營者為郵購買賣或訪問買賣時，應將其買賣之條件、出賣人之姓名、名稱、負責人、事務所或住居所告知買受之消費者。」同法第十九條之一規定，前述第十八條規定於以郵購買賣或訪問買賣方式所為之服務交易，準用之。以電子郵件為行銷方式，不論其內容是實體物之買賣或服務交易，均應依消費者保護法有關郵購買賣之相關規定辦理。依此而論，濫發電子郵件內容涉及商業性廣告者，依前揭消費者保護法之規定，利用電子郵件行銷之企業經營者有於電子郵件標題及內容揭示買賣條件、姓名或名稱等之義務，其做法即類似前章介紹外國有關立法例強制揭示電子郵件「廣告」性質之規定。

違反第十八條並無處罰之規定，似乎未克盡保護消費者之全功。但是，參酌同法第二十二條規定：「企業經營者應確保廣告內容之真實其對消費者所附之義務不得低於廣告之內容。」及第二十三條規定：「刊登或報導廣告之媒體經營者明知或可得而之廣告內容與事實不符者就消費者因信賴該廣告所受之損害與企業經營者負連帶責任。」可以推知，消費者保護法在這方面提供與消費者的保護傘並無漏洞。消費者保護法施行細則第二十三條定義前述條文中所稱「廣告」，包括了「利用電腦、電子視訊、電子語音或其他方法可使不特定多數人知悉其宣傳內容之傳播」，則對於濫發電子郵件者與委託其發送廣告之企業經營者，二者共同都需因上述規定，就其利用濫發電子郵件的商業宣傳行為，對收件者中之消費者負連帶擔保廣告內容真實之義務。消費者保護法第五十條規定之團體訴訟制度，更使可能的受害者反制濫發電子郵件行為的行動更具威力。尤其是該條第三項規定，受害者集體求償可以主張的損害賠償請求權，包括前段所述民法第一百九十五條第一項非財產上之損害，顯現出現行法律體系在因應濫發電子郵件現象的規範協調上，已具備應有的延伸性。

（二）公平交易法

1.與他人營業或服務之設施或活動混淆

國外知名網站例如PayPal及Best Buy，遭遇濫發電子郵件者仿冒以偽裝為發自各該網站的電子郵件，誘使網路使用人，在其提供的連結或依其指示路徑提供個人資料及信用卡授權號碼，藉以行騙的例子稱為”Brand Spoofing”，已經違反公平交易法第二十條第一項第二款之規定[220]；至於其他情況，例如濫發電子郵件行為人並非使用他人商號或姓名，而是隨意取一個代號來掩飾其發信來源或是變更其電子郵件地址，由於電子郵件地址(IP)是一連串的數字，非公司名稱、非姓名、亦不構成法律上定義之文書，則尚

[220] 公平交易法第二十條第一項第二款規定：「以相關事業或消費者所普遍認知之他人姓名、商號或公司名稱、標章或其他表示他人營業、服務之表徵，為相同或類似之使用，致與他人營業或服務之設施或活動混淆者。」

非本條規定禁制之列。[221]

2.虛偽不實或引人錯誤之表示或表徵

依公平交易法第二十一條之規定，事業及廣告媒體商不得於廣告為虛偽不實或引人錯誤之表示或表徵。[222]濫發電子郵件主題與內容不符，或其內容就事業廣告之商品或服務有虛偽不實或引人錯誤表示，其廣告主連同廣告媒體業都應對收件者負連帶損害賠償責任。本條禁制規定之解釋應與前述消費者保護法第二十二條及第二十三條規定意旨為相同之理解。

3.其他不正行為之禁止

公平交易法第二十四條規定，除本法另有規定者外，事業亦不得為其他足以影響交易秩序之欺罔或顯失公平之行為。本條為公平交易法所謂之帝王條款，本節開首所描述濫發電子郵件之各種態樣，若未各個落入前述公平交易法之特定條款規範範疇，亦多有可能受本條文義射程涵括，可以依個案具體事實認定「足以影響交易秩序」、「欺罔」或「顯失公平」。

實務上，行政院訴願決定台九十訴字第 0 二九五 0 七二號就美商雅虎公司(Yahoo)檢舉台灣雅虎電子商務股份有限公司，以 Yahoomall 作為英文公司名稱之特取部分網域名稱及電子郵件信箱之主要部分涉嫌違反公平交易法第二十四條之規定，所做認定，以及 2000 年行政院公平交易委員會(八九)公參字第八八〇六三八一-〇〇八號處分書，就宇江資訊有限公司以「網際萬客隆購物網站」作為電腦原文書專賣區網頁之 TITLE TAG，顯係攀附萬客隆公司商譽，增加交易機會，以達榨取他人努力成果之情事，核有足以影響交易秩序之顯失公平情事，違反公平交易法第二十四條規定，可供為本節介紹之參考。

---

[221] 余德正，前揭文，頁 137,138

[222] 公平交易法第二十一條規定：「事業不得在商品或其廣告上，或以其他使公眾得知之方法，對於商品之價格、數量、品質、內容、製造方法、製造日期、有效期限、使用方法、用途、原產地、製造者、製造地、加工者、加工地等，為虛偽不實或引人錯誤之表示或表徵。

事業對於載有前項虛偽不實或引人錯誤表示之商品，不得販賣、運送、輸出或輸入。

前二項規定於事業之服務準用之。

廣告代理業在明知或可得知情形下，仍製作或設計有引人錯誤之廣告，與廣告主負連帶損害賠償責任。廣告媒體業在明知或可得知其所傳播或刊載之廣告有引人錯誤之虞，仍予傳播或刊載，亦與廣告主負連帶損害賠償責任。」

三、實體權利之損害

濫發電子郵件之行為亦可能侵害個人或企業經營者實體法上之權利，而涉及諸如：民事侵權行為法、刑事詐欺、毀損及電腦犯罪及違反智慧財產權法等問題，茲分析如下：

【表 4.3 濫發電子郵件損害實體權利涉及之相關法律】

濫發電子郵件涉及之法律	相關規定
民法	侵權行為（姓名權、財產權）
	純粹經濟上損失（時間、金錢）
刑法	詐欺（個人法益）
	毀損（個人法益）
	電腦犯罪（個人法益）
商標法	侵害他人商標（財產權）

（一）民法

1.侵權行為

有些大量發送未經請求之商業性電子廣告信者，為規避過濾軟體的過濾阻擋，而不斷變更、偽造發信源頭與路徑，一是發信人的身分與e-mail address，二是IP address。在假造身分與e-mail address方面，如在身分設定的姓名、電子郵址、所屬組織等等欄位，擅自填入他人公司名稱商號姓名以及電子郵件地址與所屬組織等資訊，並以之散發大量電子廣告信函，則為侵害民法第十九條規定之姓名權之情形，該條除保障自然人之姓名之外，已註冊之商號亦屬之。[223]惟有學者以為，人格權受侵害時，本得依民法第一八四條第一項前段及第二一三條規定請求財產上的損害賠償，第十九條之規定不具實質意義。因此民法第十九條之規定非屬獨立的請求權基礎。[224]

依民法第一百八十四條第一項規定：「因故意或過失，不法

[223] 最高法院 20 年上字第 2401 號判例參照； 另見余德正，前揭文，頁 137
[224] 王澤鑑，前揭書，頁 140

侵害他人之權利者，負損害賠償責任。故意以背於善良風俗之方法，加損害於他人者亦同。」這裡所謂侵害權利的範圍，包括人格權、身分權、物權與智慧財產權等法律上權利。濫發電子郵件廣告之行為，對於提供郵件伺服器的ISP業者而言，雖然沒有發生物理上的損害，但是卻有可能導致網際網路服務提供者郵件寄送服務的中斷，而濫發電子郵件佔用大量的網際網路傳輸頻寬，有礙ISP業者對於其伺服器使用、收益的權能，仍屬侵權行為的一種，應對網際網路服務提供者負損害賠償的責任。國外有不少案例均承認此種民事損害的賠償責任。[225]請參閱本報告前引美國法院有關判例之介紹。

2.純粹經濟上損失

所謂「純粹經濟上損失」（pure economic loss）係指非私法上之權利受侵害，而僅受純粹財產上利益之侵害而言。純粹經濟上之損失涉及下列三項問題：

(1)在利益衡量上，純粹經濟上損失不能與人身或所有權同等比重；

(2)純粹經濟上損失之範圍，如高速公路車禍所導致之時間上損失及廢油污染致海產餐廳無法營業等，具有不確定性，正如美國法官 Cardozo 所言：「對不確定的人，在不確定的時間，而負不確定數額的責任。」（Liability in an indeterminate amount for an indeterminate time to an indeterminate class）；

(3)純粹經濟上損失尚涉及侵權行為法與契約的規範功能。[226]

就我國法制觀之，學者以為僅能於行為故意侵害他人純粹財產上利益時依民法第一百八十四條第一項後段規定，故意以背於善良風俗方法加損害於他人時，應負損害賠償責任，即以概括的方式保護純粹財產上利益。[227]至於過失責任，

[225] 賴文智、劉承慶，＜寄發廣告電子郵件的相關法律問題＞，see available at: http://www.is-law.com/OurDocuments/EC0002LA.pdf（visited on 2003/10/12）
[226] 王澤鑑，前揭書，頁 111
[227] 王澤鑑，同前註，頁 112

學說上尚有爭議。

濫發大量未經請求之電子郵件造成 ISP 業者伺服器無法負載，或造成收件者時間及勞力上之浪費，是否屬於「純粹經濟上之損失」，司法實務上尚未見有實際案例見解可供參考，本研究認為應持肯定說。

（二）刑法

1.詐欺罪

關於濫發電子郵件涉及詐欺之態樣約可分為二種：一為信件標示錯誤或虛偽不實致引人誤信而開啟；另一為信件內容以詐術使人將本人或第三人之物交付者。後者涉及詐欺罪之基本型態，應回歸一般詐欺罪之構成要件及個案具體事實認定之。而前者似因無為自己或第三人不法所有之意圖，以詐術使人將本人或第三人之物交付，或為得財產上不法之利益或使第三人得之者，縱因誤信所謂「詐術」以為其非濫發電子郵件而開啟之，亦與刑法詐欺罪所欲保護之個人財產法益尚有區別，應認不構成刑法詐欺罪之要件。

2.毀損罪

刑法第三百五十四條規定，毀棄、損壞前二條以外之他人之物或致令不堪使用，足以生損害於公眾或他人者，處二年以下有期徒刑、拘役或五百元以下罰金。惟濫發電子郵件是否將會導致電腦伺服器損壞致令不堪用，尚無實證，因此本條規定似不適用於濫發電子郵件之行為。

3.電腦犯罪專章

刑法第三百六十條規定，無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。本條之立法係規範「電腦駭客」（Hackers）侵入或破壞他人電腦之行為，濫發電子郵件之行為是否構成無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人之要件

，參閱本條文立法理由理論上可以認為已明文排除[228]。但是，本研究訪談國內ISP業者發現，濫發電子郵件的確會增加系統負載，使系統因為過多的濫發電子郵件佔據頻寬而無法提供正常服務。濫發電子郵件雖然不會對伺服器造成損害，但卻容易對儲存設備造成損害。破壞其內部資料，且無法恢復。因此，在具體個案本條規定仍有適用之餘地。

4.妨害風化罪

濫發電子郵件內容，有極高比例為色情或兒童少年不宜者。兒童及少年福利法規定，任何人不得對兒童及少年犯罪或為不正當之行為；供應有關暴力猥褻或色情之電子訊號電腦網路與兒童及少年者，處新台幣六千元以上三萬元以下罰鍰(兒童及少年福利法第三十條及第五十五條參照) 。其情節構成刑法妨害風化罪章者，亦應受追訴。

（三）商標法

濫發電子郵件係冒用他人商標以逃避他人追查信件來源或避免遭過濾軟體刪除，或標示錯誤之信件來源，並引用他人之商標(例如 ISP 業者之商標)，即係違反商標法下列相關規定。

商標法第六十一條規定商標專用權人對於侵害其商標用權者，得請求損害賠償，並得請求排除其侵害；有侵害之虞者，得請求防止之，同法第六十二條進一步就稀釋商標之情形加以規定，未得商標權人同意，有下列情形之一者，視為侵害商標權：

- 明知為他人著名之註冊商標而使用相同或近似之商標或以該著名商標中之文字作為自己公司名稱、商號名稱、網域名稱或其他表彰營業主體或來源之標識，致減損著名商標之識別性或信譽者。
- 明知為他人之註冊商標，而以該商標中之文字作為自己公司名稱、商號名稱、網域名稱或其他表彰營業主體或來源之標識，致商品或服務相關消費者混淆誤認者。

[228] 刑法第三百六十條之立法理由謂：「鑒於電腦及網路已成為人類生活之重要工具，分散式阻斷攻擊（DDOS）或封包洪流（Ping Flood）等行為已成為駭客最常用之癱瘓網路攻擊手法，故有必要以刑法保護電腦及網路設備之正常運作，爰增訂本條。又本條處罰之對象乃對電腦及網路設備產生重大影響之故意干擾行為，為避免某些對電腦系統僅產生極輕度影響之測試或運用行為亦被繩以本罪，故加上『致生損害於公眾或他人』之要件，以免刑罰範圍過於擴張。」顯見立法理由已排除規範濫發電子郵件之行為

參、 我國目前管制濫發電子郵件法制之發展現況

一、電子商務消費者保護綱領

承上節分析，我國現行法律體系對於濫發電子郵件現象帶來的問題，並非一應無解，分別就濫發電子郵件在個人資料之蒐集與利用，濫發電子郵件標題與內容之規範管制，以及濫發電子郵件在形式上對個人及企業實體上權利造成的侵害，都有相應的法律規範。但是，個別法條的操作確實需要經過論理的推敲，以及在需要保護的法益上謹慎選擇立場。因此，在適用步驟上不免會覺得有不便利之處。就此，行政院消費者保護委員會在 2002 年 11 月跨出了令人佩服的第一步，發布電子商務消費者保護綱領(行政院台九十聞字第0六三四四四號函核定) ， 把握住消費者保護的核心立場，對於濫發電子郵件現象造成的問題，統整各項相關法規的規定，建立消費者保護措施的準繩。行政院消費者保護委員會透過綱領所定之基本原則公開宣示，從事電子商務之企業經營者應尊重及維護消費者權利，並採行下列公平之商業、廣告及行銷活動：

(1)企業經營者不得進行欺騙、誤導、詐欺或不公平之商業、廣告及行銷活動。

(2)企業經營者之商業、廣告及行銷活動，不得使消費者遭受不合理風險之傷害。

(3)企業經營者應提供有關其企業本身、商品或服務之資訊，並應確保資訊之清楚、明顯、正確及易於取得。

(4)企業經營者應遵守其所訂定與消費者交易時之各項政策及措施。

(5)企業經營者不得使用不公平之契約條款。

(6)企業經營者所為之廣告內容及行銷資訊應明確，並避免與評論或其他報導相混淆，俾利消費者清楚知道其為廣告內容或行銷資訊。

(7)企業經營者應於廣告及行銷活動中明確表示其身分。

(8)企業經營者應提供消費者於行使終止或解除契約、退貨或換貨、退款之情形時，與訂購或付款時相同程度之管道與方式。

(9)企業經營者對於兒童、高齡者及其他弱勢消費者採行之廣告或行銷活動，應慎重妥適為之。

(10)企業經營者對兒童所為之廣告應避免過度誇張或引誘，並不應出現不適當之內容，如色情或暴力之圖像、文字及影音等資訊。

(11)企業經營者應考量電子商務全球化之特質，並應遵守其目標市場之各種管制措施。

(12)企業經營者不得利用電子商務之特性，隱藏其真實身分或所在位置，而藉以規避消費者保護標準或執法機制之約束。

(13)企業經營者應建立自律機制，並採行易於使用之程序，使消費者可以選擇是否希望收到其主動寄發之商業電子郵件。消費者表示不願意收到企業經營者主動寄發之商業電子郵件時，企業經營者應即停止寄發。

上述綱領對於管制濫發電子郵件雖無強制力，但是，在引導相關政府機關適用保護電子商務消費者規範，以及提供企業經營者(包括 ISP 業者)與消費者個人網際網路上商業行為準則，卻有莫大的澄清效果。

二、 電子廣告信件管理條例草案

透過單一法案的制定，尋求對濫發電子郵件問題一次性的總體解決，也已經出現在國會立法的動作中。

立法委員馮定國等人分別於 2000 年及 2002 年提案制定「電子廣告信件管理條例」[229]，其立法說明中強調：「

[229] **請參見附件二十六---** 立法院議案關係文書，院總第一七七七號　委員提案第三OO四號，馮定國立法委員提出之「電子廣告信件管理條例草案」(2000/05/24)
請參見附件二十七-- 立法院議案關係文書，院總第一七七七號　委員提案第四二八一號，馮定國立法委員提出之「電子廣告信件管理條例草案」(2002/06/01)

(1)由於網際網路的日漸普及，許多傳統商業行為也相繼運用網路的優勢，以拓展商機。在法令尚未規範下，許多網路上的商業行為實際上是對網路資源的濫用，並且侵犯所有網路使用者的個人權益，甚至成為犯罪工具，也間接阻礙網際網路的發展。

(2)以目前的網路服務費用，發送一百萬封廣告信的成本，只需從中獲得一兩筆交易即可回收，相較於傳統廣告信的成本實在是九牛一毛，因此網路上垃圾信已到了氾濫成災的地步。垃圾郵件浪費的是網路資源、收信人的時間與金錢、網路的服務品質，而發信人卻無任何損失。由於垃圾信絕大部分沒有真實的寄件人資料，更助長了網路詐欺的行為，也妨礙了網際網路整體的發展。當今政府正大力推廣電子商務，除了要有幫助企業上網的措施之外，也必須開始對妨害網路的行為加以規範。垃圾郵件是網路上諸多問題中最普遍的一種，也是最嚴重的問題之一，宜立刻立法加以禁止。」

草案全部計有十四條條文，其立法要點為：

(1)明定本條例之立法目的為避免網際網路公用資源遭受濫用維護網路服務業者及網路使用者之權益；
(2)違反本條例規定之電子廣告郵件俱屬應受管制之垃圾郵件；
(3)明定主管機關為交通部；
(4)電子廣告信件須註明發信人之名稱、地址、電話、姓名；
(5)提供發信服務之網路公司或個人必須在信件後方註明該公司或個人之名稱、郵政地址、聯絡電話、聯絡人姓名；
(6)發信人必須事先獲得收件人的同意始可發送電子廣告郵件。但收件人與發信人先前已有公務或私人的關係，不在此限；
(7)收信人可選擇不再接收某一提供發信服務公司的電子郵件；
(8)發信人或提供發信服務之公司不得以任何方式變造信件中之資料，以使收信人能明確了解發信人之資料；
(9)禁止販賣、散發、使用變造電子郵件發信紀錄之電腦程式；
(10)明定電子廣告信件之主題必須與信件內容相符；
(11)垃圾郵件之受害之個人及網路服務業者可對發信公司及代發信之業者自發信日期起一年提出賠償請求；
(12)明定收信人及網路服務公司因垃圾郵件造成之實際損失及訴訟費用均得要求發信人給予補償。[230]

[230] **請參見附件二十六-** 立法院議案關係文書，院總第一七七七號　委員提案第三OO四號，馮定國立法委員提出之「電子廣告信件管理條例草案」(2000/05/24)之立法說明

法律實務界人士對於上述草案著有批評認為，綜觀整部草案，基本上是針對濫發電子郵件一般性的問題，嘗試提出解決的方案，但是想要單純地靠立法管制來解決廣告電子郵件問題，是否在出發點上就已經存在一些盲點？怎麼界定什麼是垃圾郵件？發出幾封內容相同的信件就可以算是濫發信件？對於如何執行、法律效果、配套措施等，也沒有一個完整的設計，即便通過此一法案，恐怕也無法徹底落實。[231]

三、修正電腦處理個人資料保護法

前述「電子廣告信件管理條例」草案非常先進地採取嚴格的事前同意機制(Opt-in)規範，限制濫發電子郵件，對於保護對象之收件者也不限定於自然人用戶，更同時賦予受害之自然人及 ISP 業者起訴請求損害賠償的權利。但可惜的是，結構太過疏陋，欠缺可行性。相對於此，法務部針對 1995 年完成立法的電腦處理個人資料保護法從 2001 年起積極檢討，進行修正動作，使該法原來偏向事後拒絕機制(Opt-out)設計，一舉轉變為相當徹底的事前同意機制(Opt-in)規範，在我國有關管制濫發電子郵件的法制建構上，更加緊密了各個關係法規間的協調性及解決濫發電子郵件的有效性。

法務部在 2003 年 12 月完成的電腦處理個人資料保護法修正草案，更動現行法的幅度極大，全部草案條文共計五十三條，除將名稱修正為「個人資料保護法」外，合計修正三十三條、新增十三條、刪除五條，共五十一條，與更定新法無異。特別令人注意到與本報告主題相關的條文為修正草案條文第二十二條第二項規定，為尊重個人生活，減少不必要干擾，對於以行銷為特定目的而進行行銷時，增訂該行銷之非公務機關，應於首次行銷時提供當事人免費表達拒絕之方式；當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。儘管法務部主管官員針對本研究之提問說明，本條之將來應用係就特定人之個人資料受利用之情形所為規範，不必然可以概括適用於濫發電子郵件係針對不特定多數人，不確定是否屬於個人資料之電子郵件地址發送之情形。但是，我國管制濫發電子郵件法制進一步朝著隱私保護的核心立場鞏固，卻已經在本次電腦處理個人資料保護法修正工作成果上顯露無遺。草案新增條文規定，法務部為本法保護隱私事項的主管機關，以及參考消費者保護法成例，賦予隱私侵害事件受害人委託財團法人對侵害者提

[231] 賴文智、劉承慶，前揭文

起民事訴訟之權利，還有配合刑法新修訂有關電腦犯罪之條文，將違反本法之刑罰酌予提高；明定在我國領域外觸犯本法之罪責，亦應適用，更突出我國主政機關在本報告有關主題上亟思有所積極作為之企圖心。

四、 立法技術的考量

本研究前章有關國際管制濫發電子郵件之規範研究結果，已經鋪陳出歐盟與美國兩大市場在管制濫發電子郵件規範觀念上的重大歧異與相互較勁之處。其中差別，其實並不在究竟應該選擇事前同意機制(Opt-in)或事後拒絕機制(Opt-out) ，為反濫發電子郵件立法之基本原則，或是如何貫徹拒絕收信(Do not spam)制度之建立。歐盟有關電子通訊下保護隱私的指令，事實上是奠基在歐洲具有悠久深遠保護隱私的文化歷史，將已經在人民生活中深刻化的尊重隱私觀念，透過具體的實踐例子，一次又一次地宣示，並且拘束現代社會商業運作，防免科技發展成為脫韁野馬，對人性尊嚴及人類群體生活產生危害。在另一端成為對照的則是美國，在帶領全球經濟不斷嘗試攀爬高峰的巨大商業力量牽引下，大方且毫不遮掩地表達立場，所謂的反濫發電子郵件立法是為新興的網路直銷商業樹立全國一致遵循的規範，重點在於扶助正當的商業利益，發展健全的電子商務。我們以隱私保護、消費者保護及商業利益保護依序一字排開觀察：歐盟立法是由隱私保護展開推向消費者保護發展，美國則由商業利益保護著眼，涵攝消費者保護在其權利訴訟的巨傘下(因為資本主義經濟體制裡，顧客的權益受到保障，企業的利益才能實現) 。二者由遙遠的兩端向中間的目標消費者保護趨近而匯合。但是，在保護的手段上仍可觀察到上述觀念立場差異所形成的特殊處：在歐盟會員國，反制濫發電子郵件者的武器已經釋出給個別隱私受害的個人，但是，在美國反制及攻擊的法律工具則保留在聯邦機關、州檢察長以及 ISP 業者手上。對於電子商務及網路商業發展滿懷計劃的日本及韓國，也不例外，採取相類似於美國法的設計。當然各國有關隱私保護的法律還是在相當程度上賦予受害人個人請求救濟的權利，只不過在這一場剛興起對抗濫發電子郵件的戰爭中，讓我們更清楚看到在不同的國家政治、經濟、文化目標設定下對於不同法益的照顧程度。

(一) 增訂特別立法

馮定國委員提案之「電子廣告信件管理條例」草案點出了我國現行法律體系尚未予以明文承認的網際網路公用資源，應該成為一

項社會法益加以保障。隨之而來的則是 ISP 業者及網路使用者二者可分的權益。

本研究邀請國內ISP業者座談，關於政府應否介入並立法管理濫發電子郵件之議題，與會之ISP業者均一致反映政府修法或立法之必要性及迫切性，並且坦言目前以現行法律或定型化契約規範並無法有效解決濫發電子郵件產生的問題[232]，恰如其份顯示出制定一個特別法或特別條例將非常有助於補足現行法律體系在對於上述法益的保護上顯露的缺口。因此，對ISP業者而言，不僅得以藉由政府公權力嚇阻濫發電子郵件之盛行，更可使業者執行反濫發電子郵件措施時有法可循。就電子郵件之使用者而言，如此的特別法立法亦得以解決長期以來令人困擾之問題，並提高使用電子郵件之效率。

然而，更重要的是，由於濫發電子郵件屬於網際網路應用下之一種不正使用行為，有超國家性及無疆界性之特質，世界各先進國家也同步在整合立法方向，共同打擊濫發電子郵件。就此而論，國際合作打擊濫發電子郵件既然已經成為全球立法趨勢；加以我國網際網路應用普及度高居世界前茅，作為國際社會成員的一份子，我國實有義務儘速修法或立法，以遏阻濫發電子郵件之氾濫。

在學理上，法律的改變與發展先後可分為四個階段：

第一階段：既有規則不變，適用在新案件上；
第二階段：既有規則稍加變通後，適用在新案件上；
第三階段：為某類型的事件，制定統一規則；
第四階段：針對特定法律領域，制定新法。[233]

目前我國政府業已針對網際網路相關法律規範制度推動新增立法及修訂現行法律，包括制定政府資訊公開法、電子簽章法，並推動修正商標法、銀行法、著作權法、仲裁法、電腦處理個人資料保護法、所得稅法、稅捐稽徵法、營業稅法、刑法、電信法與有線電視法等，此外尚包括公平交易法、消費者保護法、智慧財產權法及其他民商法等。[234]網際網路相關法制之發展已確立規範基礎及框架，然而規範濫發電子郵件之管制手段，究係應在既有規則稍加變通後，適用在新案件上（如：刑法電腦犯罪專章），或為濫發電子郵件

[232] 詳見【ISP業者對濫發電子郵件之建議與期許】座談會記錄, 2003 年 10 月 3 日，見同年 10 月 14 日工商時報。
[233] 陳銘祥，＜綜論網際網路的法律規範＞，月旦法學雜誌，72 期，2001.5.，頁 155
[234] 馮震宇，＜論網路電子商務發展與相關法律問題（上）＞，月旦法學雜誌，36 期，1998.5.，頁 71

制定統一規則（如制定電子簽章法之例），甚至將來針對特定網際網路商業領域，制定新法(例如：電子商務法) ，勢將具體取決於有關立法保護對象及立法保護強度上立法者之態度。

在立法保護對象上，即使著眼於掃除濫發電子郵件對於網路商業發展及電子商務普及造成的障礙，立法者勢必需要判斷，在快速成形的電子通訊化社會中，究竟應以下列哪一個對象作為優先保護的主體:

-電子通訊的個人用戶(而且只限於自然人用戶/individual subscribers)；或
-電子通訊的企業用戶(公司組織內成員是否一併包括?) ； 或
-ISP 業者。

上述選擇結果，必須事先考量各個應受保護法益在執法最大可能成效內，可以獲得的保護效益，以及可能的正面擴散效應，例如國家資訊通訊安全、社會交易秩序以及擴大消費者對電子商務信心，加以比較，而搭配適宜的立法保護強度例如：

-誰可以請求排除侵害及賠償損害?
-採取民事訴訟、刑事訴訟或行政救濟手段?
-法益平衡如何獲得適當的確保?

上述思維，依循電子通訊社會快速普及程度的提昇，一路發展下來而具像為嶄新的法律規範出現時，負責推動及執行這個大型的社會法制改造計劃的主管機關，不可避免必須在相關的技術處理能力上具備優勢的強項，以貫徹法定應有的作為。由此看來，若以選擇制定新法為處理本研究主題之法律上方案，則性質上較適宜為法定主管機關者，可能將是預定在 2004 年年底前正式成立的通訊傳播委員會。

(二)修正現行法令

以濫發電子郵件，在形式上及內容上顯現的商業性，對於使用者產生隱私權及電子商務交易安全之騷擾與侵害，現行法令關於保障個人隱私權及維護交易安全者，包括電腦處理個人資料保護法、消費者保護法及公平交易法都應是可資立即應用，而發揮預期保護效果者。

謹以下表整理例示可以參考進行的修法作為：

表 4.4 建議修正現行可適用於管制濫發電子郵件的法律

濫發電子郵件可能涉及之法律	相關規定	建議修正條文	備註
電腦處理個人資料保護法	「個人資料」之定義	足資直接或間接識別該個人之資料均應包含之，且應明確規定電子郵件地址屬於「個人資料」之情形及適用範圍。	法務部草案已修正
	適用之範圍	不僅應廢除行業別之限制，同時應不限於電腦之應用始足當之。	法務部草案已修正
	維護個人資料之義務	蒐集資料時不論是直接或間接蒐集，除符合得免告知情形者外，均須明確告知當事人蒐集目的、資料類別、資料來源等相關事項。	法務部版草案已修正
	販賣個人資料之處罰規定	建議增列非公務機關（如網路商家）販賣個人資料之罰責及其損害賠償責任。	法務部草案已修正
	其他	應增列禁止廣告電郵寄自網站下載之 email 或以隨機軟體自動組合 email 等類似規定，且電子郵件名單應合法取得。	

公平交易法	不正行為禁止之規定	應增列商業性電子郵件內容有虛偽、錯誤或引人錯誤者，亦為公平交易法之處罰範圍。	
		關於公平交易法第二十四條「足以影響交易秩序之欺罔」或「顯失公平之行為」，對於濫發電子郵件應有適用。	
消費者保護法	郵購買賣之相關規定	應明確規定商業性電子郵件須明示「廣告」之性質；如內容有色情之資訊，應於信件標題標明「成人」。	
		應揭露商業性電子郵件之發信來源、發信人名稱、姓名、地址、電話等資訊，並增列未依消保法第十八條標示之處罰規定。	
		商業性之電子郵件內應有使收信者表明或註冊拒絕接收該發送人信件之方式及設計。	
		應增列賠償消費者之規定。	

1、電腦處理個人資料保護法

法務部於九十二年十二月間完成電腦處理個人資料保護法修正草案，其總說明謂：「為規範電腦處理個人資料，避免人格權受侵害，並促進個人資料之合理利用，法務部於七十九年間參酌『經濟合作暨發展組織』（OECD）所揭示的保護個人資料八大原則，研擬制定『電腦處理個人資料保護法』草案，經完成立法程序後，於八十四年八月十一日由 總統公布施行迄今。惟因電腦科技的日新月異，利用電腦蒐集、處理、傳輸個人資料之情形日漸普遍，對個人資料隱私權益之保護，造成莫大之威脅。尤其該法對非公務機關有行業別之適用限制規定，又有諸多不確定法律概念，對個人資料之保護，確有不周延之處，實務上亦發生許多窒礙難行之困難。」因此法務部研擬修正部分條文，除放寬個人資料之範圍，除自然人之姓名、出生年月日、身分證明編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動外，增訂其他足資直接或間接識別該個人之資料；此外，刪除非公務機關行業別之限制，即任何自然人、法人、機構或其他團體，除單純為個人或家庭活動之情形外，皆須適用本法（修正條文第二條、第七條）；增訂蒐集資料時不論是直接或間接蒐集，除符合得免告知情形者外，均須明確告知當事人蒐集目的、資料類別、資料來源等相關事項（修正條文第九條）。

本研究建議，除前述修正草案規定外，為維護電子通訊社會中個人隱私權，本法宜明訂個人使用之電子郵件地址在何種情形下可以成為本法保障之個人資料，另外，增列禁止廣告電郵寄自網站下載或其他不正當方式獲知之email或以隨機軟體自動組合email等類似規定，且電子郵件名單應合法取得。

2、公平交易法

按公平交易法第二十一條規定，已明確禁止事業為虛偽不實記載或廣告，並課予廣告代理業、廣告媒體與廣告主應負連帶損害賠償責任。本研究建議，本法應明確增列事業利用電子郵件作為行銷方式時，如信件之信件標題、來源、發信人資訊等內容有虛偽、錯誤或引人錯誤者，亦應為公平交易法之處罰範圍，當更為允洽。

此外，公平交易法第二十四條雖規定：「除本法另有規定者外，事業亦不得為其他足以影響交易秩序之欺罔或顯失公平之行為。」然而，

由於濫發電子郵件係將行銷成本轉嫁予 ISP 業者及收信人，或以成本低廉之大量發信軟體發信，致其他業者造成損害，而發信人則獲取顯不相當之利益，由 ISP 業者及收信人負擔不必要之成本，已成為目前普遍之情形；尤有甚者，濫發電子郵件將對以其他正當行銷方式但花費較高之事業形成不公平競爭，造成惡性競爭；因此，為遏止濫發電子郵件所造成之不公平競爭行為，本條規定有必要使濫發電子郵件之行為納入規範，爰建議於本法施行細則適當增列解釋為不公平競爭之情形之一，並應有第二十四條之適用。

3、消費者保護法

（1）應強制規定企業經營者揭示大量發送廣告電子郵件來源及性質

本研究建議，應修正本法第十八條之規定，強制標示企業經營者揭示大量發送廣告電子郵件來源及性質：且除第十八條原列舉之項目外，應明確規定電子郵件廣告明示「廣告」之性質；如內容有色情之資訊，應於電子郵件標題標明「成人」。

本法並未規定違反第十八條揭示義務規定時應如何處罰，宜規範之，加強管制之效果。

（2）應賦予消費者表明拒絕收受濫發電子郵件之權利

本研究建議，本法配合電腦處理個人資料保護法之修正，增訂電子郵件廣告內應有使收信者表明拒絕接收該發信人郵件之方式及設計。

（3）應增訂賠償消費者之規定

除本法應明確規定對於濫發電子郵件之處罰方式外，對於因此致消費者受損害者，本研究建議，增訂法定賠償制度，併納入本法原已規定之消費者損害賠償訴訟與消費者集體訴訟制度範圍(消費者保護法第五十條至第五十四條參照)。

4、電信法

濫發電子郵件造成的電信網路利用效率降低，甚至相關儲存設備損害，影響所及，並不只是國民及網路使用者近用基礎網路設施

行使資訊自由權利遭到侵蝕而已，因為濫發電子郵件往往不當利用網際網路開放架構及 open relay 功能,導致各國 ISP 業者相互防堵網路上大量突發流竄的濫發電子郵件，損及整體網路交易及跨國商業資訊傳輸安全，更是嚴重。減少或消除這種不公平的濫用公用資源現象，可以考慮在電信法中增列規定，賦予電信事業排除濫發電子郵件所生侵害，以及對特定已知形成中侵害賦予電信事業防止請求權。

五、小結

綜前所述，我國法律對於個人隱私之保障、交易安全之維護及侵權損害賠償之法制均已粲然大備。針對濫發電子郵件此等新興之行銷方式引發之爭議問題是否應制定特別法，另加規範，各界意見紛陳。惟就維持我國法制均衡秩序，兼顧提振電子商務交易發展之政府施政目標，似以修正現行法律已足妥適。本研究以為，修正目前之電腦處理個人資訊保護法、消費者保護法及公平交易法等法律，併斟酌增訂條文於電信法，賦予電信事業在一定情形採取防免濫發電子郵件行為，實質上應已大致符合目前國際上關於管制濫發電子郵件之規範內容及立法趨勢，並足敷規範目前濫發電子郵件之亂象。惟立法技術上，由於上述法規修訂須分別經過提案修法手續，恐有緩不濟急、未克同時銜接之疑慮，且對於打擊濫發電子郵件而言，有無法畢其功於一役之憾，故另行制定特別法亦為可行之行動方向。目前立法院已見立法委員提案，雖已略具雛形，惟仍多嫌疏陋，如有必要制定特別法，宜參照各主要先進國家之法令規範，以完善制定符合我國國情及適當促進國際合作之法律。

第五章　結論與建議

壹、研究發現

為了能夠清楚描述本報告所謂未經請求任意發送之電子郵件現象，本研究將有關此現象之眾多定義大約歸納成下列兩種：不請自來的大量電子郵件（unsolicited bulk e-mail，簡稱為 UBE），以及不請自來的商業電子郵件（unsolicited commercial e-mail，簡稱為 UCE）：

-「不請自來的商業性電子郵件」（UCE，unsolicited commercial e-mail），係未經收件者事前許可或同意，就逕自對其大量遞送內容為商業性質的電子郵件，類似於一般常見的投寄至家庭或企業信箱的某些直銷刊物，同樣都是未經收件者的同意而寄發郵件，不同的是，在前者較難查出此郵件是否為未經請求而寄送的郵件。

-「不請自來的大量電子郵件」（UBE，unsolicited bulk e-mail），同樣是未經收件者事前許可而對之大量寄送的電子郵件，強調的是數量，而非郵件的內容(不僅僅限於商業廣告，其他諸如宗教性、政治性、問卷形式、種族議題、色情等等皆包括在內)，由於發信人往往在短時間內寄發大量電子郵件，經常造成 ISP 業者網路系統設備負擔過重甚而出現當機情形。

本研究將上述「不請自來的商業性電子郵件」（UCE）定名為「濫發電子郵件」。對其描述，包含以下數個或全部特徵：

-濫發電子郵件通常是經過自動化機器產生而大量傳送；
-濫發電子郵件發信人通常是匿名或掩飾其真實發信地址；
-濫發電子郵件之發送對象為多數不特定收件者，甚至收件之電子郵件地址有時未必真實存在；
-濫發電子郵件之發送通常未經各個收件者事前同意；
-濫發電子郵件之訊息內容為商業性，不屬於政治、宗教、教育或文化目的者；
-濫發電子郵件內容為虛偽不實甚或違法者；
-濫發電子郵件往往沒有提供有效的回覆拒絕機制，使收件者可以拒收後續接踵而來的郵件。

針對上述濫發電子郵件現象，本研究有如下發現：

一、濫發電子郵件現象日趨氾濫

相較於國際知名電子商務研究機構披露，濫發電子郵件數量急速成長，在 2004 年可能達到全球電子郵件總數量的五成以上，目前台灣的網路使用者數目以每年增加將近一百萬人的速度成長，然而對於濫發電子郵件行為感到困擾的比率，也由 2002 年僅佔所有網路使用人口的 7.4%，攀升到 2003 年的 11.8%，其成長幅度高達 59%。根據市場研究公司估計，網路使用者對網路上濫發電子郵件氾濫感到困擾的比例，在 2004 年可能更高達 50%以上。另外，在網路使用行為的主要困擾上，2003 年的實證調查數字顯示，也有高達 26.5%的上網人口對垃圾資訊太多感到不滿，顯示在台灣網路使用越來越普及的情況下，濫發電子郵件行為造成的影響程度，正在逐步升高。台北市消費者電子商務協會所做一項尚未經證實的調查估計則透露，我國每年得花費新台幣六百億元以上的社會成本來處理濫發電子郵件。

二、個人用戶隱私受侵害

台灣終止童妓協會在 2003 年 10 月委託蕃薯藤入口網站，進行網路調查發現，78%網路使用人每週都會收到色情訊息；而發生在鄰國日本及韓國濫發手機簡訊影響使用人權益的情形，在我國也日益嚴重。交通部電信總局 2003 年 12 月發布資料顯示，我國每年約有二億通的簡訊使用量，其中有約 10%，即二千萬通為詐財內容之簡訊。綜合上述網際網路使用者與行動電話使用者面臨濫發電子訊息威脅之處境，濫發電子郵件不僅已造成使用者之困擾，其背後所隱含對於隱私權的侵害更不容小覷。

三、ISP 損失報告

鉅量的濫發電子郵件損壞電腦之儲存容量，也降低電腦間與線上文件儲存或運輸速度，迫使網路服務提供業者（ISP）必須花費數百萬元建置額外的電腦裝置或聘僱處理人員來處理相關之問題。收件者及一般公司行號為阻擋濫發電子郵件，因此被迫購買過濾

濫發電子郵件之軟體，但是因為濫發電子郵件發信人往往非常狡猾，這樣的軟體通常只能過濾部分的信件，有時候甚至會過濾到非不請自來的郵件。

我國國內 ISP 業者雖然尚未有具體實際損害報告，但是，依據 ISP 業者投資軟硬體設備，網路消耗頻寬及人力成本估算，平均處理每封濫發電子郵件成本約新台幣 0.02 元，每年約達新台幣 300-350 萬元。此成本包括頻寬、人力及系統軟硬體等成本，並僱請專責人員或成立 SPAM 處理小組(包含客服及系統管理等專職人員任務分組)。

對於 ISP 業者而言，為了維持網路系統正常運作，必須加大頻寬、安裝新的過濾軟體程式以及撥用更大的容量以接收全部郵件，而這些花費最後勢必轉嫁到消費者身上，可能在未來造成消費者使用率的降低。除此之外，濫發電子郵件甚至成為阻礙網路發展的元兇，以台灣學術網路為例，濫發電子郵件的大量傳送，佔用網路頻寬成為網路塞車的最大禍首。在網際網路上不斷變更路徑及發信郵件地址的濫發電子郵件，也引發了不同國家 ISP 業者之間窮於奔命，應付瞬間突增的網路流量，甚至，相互將對方伺服器位址列入黑名單，試圖阻擋多數不收歡迎的濫發電子郵件。如此一來，反而影響正當電子郵件的跨國傳送，影響正常交易進行。

四、立法管制已經為國際趨勢

（一）歐盟的積極立法作為帶動全球規範濫發電子郵件之立法風潮從歐盟 Direcive 97/66/EC「電信部門下之個人資料處理及隱私權保護指令」、Direcive 2000/31/EC「資訊社會各項應用服務中內國市場電子商務之法律議題指令」到 Direcive 歐盟立法規範及其標準帶動各國立法風潮：2002/58/EC「電子通訊中個人資料處理及保護個人隱私指令」一路發展下來，我們看到，歐盟完整以隱私保護為軸心建構的網路秩序規範，透過其指令實施的強制，漸次統合歐洲各個經濟強權，在網際網路新紀元處理濫發電子郵件現象所帶來多項交錯複雜的權益衝突問題的共同立場，進而擴張其影響力到各個重要的國際組織，包括聯合國及經濟合作發展組織，呼籲世界其他國家採取與歐盟相同或貼近之立場，以縮短國際合作解決濫發電子郵件問題所可能耗費的冗長溝通時間，儘速建立有

效遏止濫發電子郵件現象繼續擴大蔓延的執行機制。歐盟執委會針對美國國會在討論 CAN-SPAM ACT 法案之際，積極遊說美國採取相同的事前同意機制，尤其顯示歐盟在本議題上擔任火車頭帶領國際立法風潮的決心。歐盟執委會負責企業與資訊化社會事務的委員 Erkki Liikanen 強調，各國政府必須趕在濫發電子郵件摧毀全球使用者對於網際網路及行動通信網路的信心之前，全面對濫發電子郵件者宣戰。其具體戰略則是各國應盡量依相同標準來管制濫發電子郵件，不使濫發電子郵件者有機可乘，鑽營各國管制法令漏洞，繼續對網際網路使用秩序造成威脅。長遠看來，歐盟各國在廣大的歐洲市場以歐盟指令作為其國內規範濫發電子郵件之立法依循，極有可能影響其他研究制定管制濫發電子郵件法律的國家，仿傚歐盟指令立法之結構與方式做為其參考之指標。

（二）Opt-in 與 Opt-out 機制之取捨

美國 CAN-SPAM ACT 立法，在微軟公司領軍由直銷協會(Direct Marketing Association)出面積極遊說國會，就管制濫發電子郵件立法確定採取事後拒絕機制(Opt-out) ，在這個維護商業利益立場上進行遊說的利益團體並不掩飾，其憂懼重新再有起色的網路商業在對抗濫發電子郵件者的法律戰爭中，一併和不法的行銷業者陪葬，而積極動員國會議員朝其希望維持既有網路行銷模式，但消除網路匿名效應的設計提案。但是，美國 CAN-SPAM ACT 採取事後拒絕機制立法管制方式，對於亞洲的日本與韓國等前已確立採取事後拒絕機制反制網路上濫發電子郵件行為的國家，似乎是更提醒他們，在隱私保護之外以推動全球化網路商業為國家發展目標的政府，不宜輕言犧牲或因此延緩重商主義實踐的腳步。

與此相對的是，歐盟立下典範的事前同意機制(Opt-in) ，管制所有商業及電子郵件發信人，在取得收件人事前明示同意之前不得發送商業性質之電子訊息。澳洲緊隨歐盟立法腳步，也採取相同原則完成立法。理論上，事前同意機制對於收件者個人隱私提供之保護程度應該遠高於事後拒絕機制。但是，實踐上，各個國家立法並未嚴格地或徹底地傾向採取事前同意機制或事後拒絕機制。採取事前同意機制立法的國家，包括英國及歐盟其他會員國，甚至澳洲都在所謂事前同意的定義上，開闢例外緩和正常商業活動可能受到的不便和阻礙，實際上變成一種妥協的事前同意機制，而採取事後拒絕機制立法的國家，例如

美國及韓國，若不單以立法內容評斷，而一併檢視其執行做法及相關配套措施，包括民間 ISP 業者與消費者保護團體積極動員反制濫發電子郵件的活動情形，似乎結果上並不遜於事前同意機制實施的成效。時間終究會證明孰能擅場。

（三）其他利用自動系統傳送訊息的行銷方式亦逐漸納入規範：

從第三章所述各國最新法制發展中，我們可以看到，歐洲各國因為歐盟指令之規定，大部分國家已經將利用自動電話系統撥打不請自來的電話納入規範中，規定電話撥打者應於打電話之前取得受話者之同意，甚至在奧地利、丹麥、瑞典及比利時等國家，已將其規範範圍擴張到對於任何利用自動系統傳送之廣告訊息，皆須受到這些法規的規範，無論這些訊息是以電子郵件、傳真、手機簡訊或電話等形式出現。而日本在其特定電子郵件法及特定商業交易法之相關規定中，除了規範以電腦收發的信件，還包括以行動電話收發的廣告電子郵件。由此可知，同樣基於保護消費者個人資料免於洩漏的危險，以及使現代科技不致淪為業者行銷濫用的手段和消費者的夢魘，將其他利用自動系統傳送訊息的行銷方式一同納入管制範圍，將成為未來之管制發展趨勢。

（四）立法管制濫發電子郵件之後續作為：

雖然立法管制濫發電子郵件問題已經成為各國法制上的趨勢，然而以美國的情形來看，即使該國國內有超過三十州訂立州法管制濫發電子郵件問題，美國仍然是世界上濫發電子郵件之最大來源國，由此看來，光靠立法管制尚無法達到有效的控管目的，使濫發電子郵件問題從此消失，立法並非解決濫發電子郵件問題的萬靈丹，在法律的執行上還是得面對濫發電子郵件者隱藏 IP 位址，以致追蹤困難以及逃至國外規避法律等等難題。因此，在立法規範濫發電子郵件問題之後，世界各國政府乃至於民間網路服務業者仍須持續關注此一問題，並擬定長遠計劃共同對抗，才能收到遏止之效。而這些與立法執法做為配套的方法包括：發展科技方面的防制手段、教育業者及消費者正確的行銷做法與處理電子郵件接收的保護準則，以及國際合作遏阻濫發電子郵件蔓延。

貳、建議

本研究根據以上發現，及研究期間所蒐集分析之豐富資料歸納得出結論：濫發電子郵件帶來的問題，並不是只有一個；完全禁絕濫發電子郵件現象，事實上並不可能。但是，在一定期間內有效減少濫發電子郵件之數量，以及遏止濫發電子郵件散佈之不法內容與電腦病毒，確實可能透過執行適當法律，鼓勵網路服務業者採取積極預防作為，以及教育企業經營者與消費者正確看待網路行銷的觀念來實現。貫串這一種多管齊下模式而奏功的關鍵，則是多邊的政府間國際合作。

本報告謹提出建議如下：

一、以濫發電子郵件，在形式上及內容上顯現的商業性，對於使用者產生隱私權及電子商務交易安全之騷擾與侵害，現行法令關於保障個人隱私權及維護交易安全者，包括電腦處理個人資料保護法、消費者保護法及公平交易法都應是可資立即應用，而發揮預期保護效果者。進一步修訂現行保護隱私及交易安全的法令，將保護擴及於制止濫發電子郵件可能帶來的實害及經濟損失，並考慮賦予 ISP 業者法律上權利，阻止濫發電子郵件散佈，應足以形成符合國際水準適當的規範體系。

二、惟立法技術上，由於上述法規修訂須分別經過提案修法手續，恐有緩不濟急、未克同時銜接之疑慮，且對於打擊濫發電子郵件而言，有無法畢其功於一役之憾，故另行制定特別法亦為可行之行動方向。制定一個特別法，將非常有助於補足現行法律體系在對於上述法益的保護上顯露的缺口。對 ISP 業者而言，不僅得以藉由政府公權力嚇阻濫發電子郵件之盛行，更可使業者執行反濫發電子郵件措施時有法可循。就電子郵件之使用者而言，如此的特別法立法，亦得以解決長期以來令人困擾之問題，並提高使用電子郵件之效率。制定特別法，可以在隱私保護的角度之外，著眼於通訊安全與國家電信基礎建設之維護，置重處理濫發電子郵件產生濫用網路公用資源侵害社會法益與個人法益之問題，而宜規定下列事項：

（一）建立認定濫發電子郵件標準；
（二）如何禁止發送濫發電子郵件；

（三）賦予網路使用者拒收選擇權，以採事前同意機制(opt-in)為宜；
（四）廣告主及發信人應於電子郵件納入"商業"或"廣告"等標示，以利收件者選擇過濾；
（五）ISP業者主動或被動之義務過濾；
（六）虛偽發信來源或規避行為之防制；
（七）強制廣告主提供真實資訊，例如正確發信來源與聯絡方式，俾收件者回覆、爭訟或提出要求；
（八）損害賠償額度、舉證責任分配及研析禁止騷擾性訴訟可能性；
（九）發送濫發電子郵件行為犯罪化之優劣研析；
（十）管轄權與審判地決定；
(十一) 國際合作之促進與必要授權。

三、立法管制範圍暫先只限於網際網路上濫發電子郵件之散佈。對於行動電話網路上已出現或可能濫發之廣告簡訊，目前市場收費機制以及電信業者配合主管機關督導所實施的防制措施，已見成效，本報告建議可以保留觀察。

四、成立專責主管機關積極參與國際合作。從濫發電子郵件之本質為行銷行為觀之，我國主管濫發電子郵件之專責主管機關似乎應為公平交易委員會（例如在美國為聯邦貿易委員會負責）。但依循電子通訊社會快速普及程度的提昇，一路發展下來而具像為嶄新的法律規範出現時，負責推動及執行這個大型的社會法制改造計劃的主管機關，不可避免必須在相關的技術處理能力上具備優勢的強項，以貫徹法定應有的作為。由此看來，若以選擇制定新法為處理本研究主題之法律上方案，則性質上較適宜為法定主管機關者，可能將是預定在 2004 年年底前正式成立的通訊傳播委員會。不論如何，專責隱私保護主管機關(依將來修訂完成之個人資料保護法，將是法務部及各目的事業主管機關)在本主題上，與上述經決定後之主管機關並肩工作，一起投入與鄰國及世界主要市場間之多邊規範或合作方案協調，勢必不可或缺。當務之急尤應立即回應亞洲太平洋地區已經對我國表達合作打擊濫發電子郵件誠意之國家，建立共通行動準則。