處理未經收件人許可而發出的電子訊息問題的諮詢文件

引言

1. 電訊網絡經已成爲無分國界的通訊媒介，獲商界和整體社會廣泛採用，當中尤以互聯網爲然。現有的資訊通訊科技爲拓展商機帶來巨大潛力，並可減省成本、提高效率和改善質素，更有助小型企業更多積極參與全球商貿。雖然電訊網絡帶來接通世界的新機遇，但同時亦令人們得以收集大量個人和機構的電子郵件（電郵）地址、傳真號碼和流動電話號碼等聯絡資料，並透過電子媒介，例如電子郵件或傳真，可以幾乎分文不費地迅速傳遞資訊，與傳統的直接促銷郵件方式截然不同。

2. 隨著科技發展，電郵的使用成爲非常方便的傳送訊息的方法。目前，電郵是未經收件人許可而發出電子訊息的最常見方法。使用公共網絡傳送大量未經收件人許可的電子郵件往往被稱爲「濫發電郵」，有關郵件則被稱爲「濫發郵件」。大部分未經收件人許可而大量發出的電郵均屬商業性質，用作宣傳產品或服務，可被視爲傳統上未經收件人許可而發出的郵件及其他直接促銷手法的延伸。廣義而言，濫發郵件亦可有其他形式，例如，以較傳統方式透過傳真發出未經收件人許可的電子訊息，對一些收件人造成滋擾的問題仍然存在。此外，透過流動電話短訊服務及多媒體訊息服務發出未經收件人許可的宣傳訊息的問題亦有所增加。

3. 本諮詢文件旨在研究各種濫發郵件方式所帶來的問題、目前處理未經收件人許可而發出電子訊息問題的方法的效用、以及討論解決有關問題的可行方法，包括制訂法例和加強現有指引／實務守則的適切性。

4. 政府留意到，推行額外的未經收件人許可而發出電子訊息的規管措施，勢必令有意從事直接促銷或電話促銷的人士的成本增加，以符合有關措施的規定，而成本的多少取決於規管類型和其他因素。儘管如此，當局考慮是否引入額外規管時，會同時考慮對促銷從業員的影響、對濫發訊息收件人、互聯網服務供應商及流動服務供應商等的成本影響／滋擾程度，以及執行的成本效益。政府瞭解到，應在濫發郵件活動對社會和經濟的影響，以及電訊網絡作爲普羅大眾及商界的通訊媒介的效益和效率之間取得適當平衡。

濫發郵件的定義

5. 我們在研究解決未經收件人許可而透過電子媒介發出訊息問題的適當規管措施前，有需要先行界定規管措施所要針對的問題。

電子訊息

6. 除濫發電郵外，未經收件人許可的「電子」訊息亦可透過短訊服務、多媒體訊息服務、傳真及話音信箱發出。隨著流動電話在香港日趨普及，透過流動電話短訊服務和多媒體訊息服務濫發促銷訊息的情況亦愈來愈普遍。現時，雖然一般認爲透過短訊服務和多媒體訊息服務濫發訊息的情況比濫發電郵輕微，但隨著流動電話的使用增長及資訊通訊科技的發展，規管架構應該適用於以上範疇和技術中立。規管架構應包括電郵及透過其他電子媒介發出的訊息，例如短訊服務和多媒體訊息服務等，冀能與技術發展同步前進。

7. 雖然濫發訊息的關注焦點轉移至濫發電郵、短訊和多媒體訊息，但透過較傳統的傳真方式發出未經收件人許可的電子訊息的問題亦不容忽視；本地固定電訊網絡服務（固網服務）營辦商於二零零三年就共收到 24 232 宗有關投訴。爲制訂適當的規管措施，「濫發郵件」一詞因此亦應包括未經收件人許可而發出的傳真訊息。

未經收件人許可

8. 幾乎所有濫發郵件活動的關鍵問題均在於有關電子訊息必是「未經收件人許可而發出」。一般而言，如收發訊息雙方之前沒有任何聯繫，收件人亦未曾明確同意接收訊息，有關訊息即可被視爲未經收件人許可而發出。這項定義亦包括之前已要求終止聯繫的收件人，他們通常曾指示發送一方日後不要再傳遞任何訊息。

9. 值得注意的是，「不需要」的訊息可能並不一定等同於「未經收件人許可而發出」的訊息，因爲收件人之前可能曾經同意接收有關訊息。雖然部分市民認爲，所有廣告或甚至所有不需要的訊息均屬濫發郵件，反濫發郵件人士一般卻認爲濫發郵件只限於收件人未有同意接收的訊息。

10. 發出商業訊息是否需要收件人事先許可，是一個常見的爭論點。「許可」本身亦有不同程度。一方面，收件人在收到商業訊息前可能已明示同意 (有時稱爲「opt-in」 — 「選擇接受」)；另一方面，收發雙方可能早已存在業務關係，當中隱含同意。在這情況下，除非收件人主動通知發件人無意收取有關訊息，否則發件人可隨意發出商業訊息。有其他意見稱，促銷公司應有權宣傳其產品或服務。商業訊息的發送可毋須事先取得收件人許可，但條件是收件人必須有方法選擇日後不再接收訊息，一般稱爲「opt-out」 — 「選擇不接受」。

11. Asia Digital Marketing Association (ADMA) 在「*Asia Digital Marketing*

Association 對打擊濫發郵件法例的立場文件」(http://www.asiadma.com/downloads/guidelines/pdf/100040/Position_of_the_ADMA_on_legislation_to_fight_spam.pdf)中，提倡經事先許可的電郵促銷方法，以協助打擊濫發郵件及保證消費者只會收到他們感興趣或相關的資訊。ADMA 發出*負責任的電郵促銷指引*，推廣經事先許可的電郵促銷活動。

商業

12. 「商業」一般是根據訊息內容界定，與發件人是否具實際或假定意圖無關，並涵蓋「直接」及「間接」促銷活動。標準的定義爲包括任何促銷產品或服務的訊息，但要作出包含所有可能性的定義，是非常困難或甚至不可能的。因此一般傾向採用一個簡單的定義，但同時列明不會被視爲「商業」的例外情況。

13. 澳洲的《2003 年濫發電郵法》規定，法例所涵蓋的訊息須屬於「商業」性質 – 即有關訊息是提出商業交易、或指示收件人前往進行商業交易的地點。對「商業」下定義使法例得以打擊屬於欺詐性質的濫發郵件。另一方面，美國的《2003 年 CAN-SPAM 法》將「商業」電子訊息界定爲「任何商業廣告或用以促銷產品或服務的電子郵件訊息」。

大量

14. 濫發郵件的真正問題往往在於發給收件人的電郵訊息數量。故此，濫發郵件有時指未經收件人許可而大量發出的電子郵件。發送單一訊息給大量收件人明顯符合這定義。同樣道理，將相同的訊息分別發給大量收件人，亦被視爲大量發送；大體相同的訊息及單一訊息的複本亦可能符合「大量」的定義。「大量」的定義，目前並無公認的上限 – 須視乎個別情況而定。

問題的性質

不良內容

15. 濫發郵件涉及多項問題，而不少反對濫發郵件的意見均與內容有關。由於有相當數量的濫發郵件載有不法內容，因此明顯引起關注，包括宣傳色情、非法賭博服務、層壓式推銷法、賺快錢計劃，或具誤導性和欺騙性的業務手法。

侵犯個人私隱及對消費者造成滋擾

16. 濫發郵件對消費者造成滋擾。收集和處理電郵地址及個人資料的手法涉及多

項重要的私隱權問題，例如，部分受消費者詬病的常見收集地址方法包括電郵地址收集者暗中從互聯網收集地址、在用戶瀏覽部分互聯網站時收集資料，並於未經擁有人知悉或同意的情況下大量買賣所收集得的電郵地址。很多濫發電郵者沒有向用戶提供取消「許可發送」的選項；其他投訴人則表示，即使有取消「許可發送」的選項，卻沒有效用，或甚至成爲有關電郵地址有效及使用中的確定，最終招致更多濫發郵件。

17. 有投訴指出，濫發郵件令電郵儲存量超額，因而招致額外費用。部分投訴電郵儲存額外費用的人士表示，電郵帳戶內未被刪除的濫發郵件導致高達 2,000 元的應計儲存費用。

18. 此外，有部分流動電話用戶投訴在未經他們許可的情況下收到短訊。

19. 至於住宅傳真方面，有傳真用戶徹夜收到促銷傳真，浪費大量紙張。部分濫發傳真者使用經由軟件程序自動產生的號碼，並將傳真訊息送往該等經由軟件程序自動產生的號碼，而毫不理會該等號碼的使用者是傳真、住宅或流動電話用戶。收到「傳真音頻」的流動電話用戶不但備受滋擾，更會浪費通話時間。住宅電話用戶亦受到「傳真音頻」的騷擾。

對商界造成的問題

20. 未經收件人許可而發出的電子訊息令工作人員的生產力損失、令商界需要提高網絡容量（就濫發電郵而言），亦會浪費其他資源。商界受到若干種類的濫發郵件襲擊時，更需要耗用資源進行保安調查。

21. 未經收件人許可而發出的電子訊息的人士有時會在訊息的「寄件人」標頭或其他地方填上正當公司的名稱，令人以爲訊息是來自著名的公司或得到他們的許可。這些正當公司的商譽因而受損。

22. 未經收件人許可而發出的電子訊息經常影響正當公司促銷產品的方法。以電郵而言，很多消費者加入著名公司的許可發送電郵名單，以接收特惠折扣資料、減價或新產品的通知。然而，這些電郵有時會被過濾產品或收件人誤爲濫發郵件。

網絡問題

23. 無論內容如何，濫發郵件佔用大量頻寬及儲存空間，對互聯網服務供應商造成損害，亦會滋擾客戶及增加技術支援的成本。爲打擊大量發出的電郵，互聯網服務供應商需要建立龐大的系統容量；電郵量增加，亦會大幅減低互聯網速度、

令伺服器過載及對系統穩健性造成威脅。

24. 部分濫發郵件者並不收集真正的地址，而是試圖在熱門域名使用常見名稱或各種字母的組合。這對互聯網服務供應商的伺服器造成重大壓力，因爲無數電子郵件被發出，而發給不存在的電郵地址的訊息亦會被退回。

25. 濫發郵件者有時會使用匿名轉發的方法，從而掩飾訊息來源、轉移投訴目標、規避其他網絡的「反濫發郵件」措施，以及增加可發送的訊息數量。第三者轉發通常意味著服務遭受盜用，因爲這是未經授權的挪用電腦資源行爲。第三者轉發耗用頻寬及儲存容量，可以導致表現質素下降，甚至系統失效。最高昂的成本通常來自工作人員處理被退回訊息、投訴和重組系統所需的時間。

濫發郵件者使用的其他方法

26. 僞冒訊息標頭，亦是濫發電郵者常用的技倆。濫發郵件往往令憤怒的收件人作出大量投訴。故此，濫發郵件者使用各種手法轉移投訴目標，例如在訊息標頭使用虛假的回郵地址，並往往於訊息內提供虛假的「拒絕接受」電郵地址。

問題的嚴重性

27. 一如上文討論，濫發郵件有多種形式，視乎所用的傳送技術而定。雖然目前濫發傳真及濫發電郵的問題比濫發短訊及多媒體訊息嚴重，但由於技術新發展令發送短訊和多媒體訊息的成本有所下降，這問題愈來愈值得關注。

電郵

28. 香港互聯網供應商協會於二零零三年十二月就濫發郵件問題進行調查，向 11 家服務香港超過 90%的互聯網用戶的互聯網服務供應商收集數據。假設濫發郵件包括未經收件人許可而發出的商業電郵和大量電子郵件，該調查發現香港互聯網服務供應商所處理的全部電子郵件當中，有 50%屬於濫發郵件，其中 5%是來自香港，另有 20 至 40%是來自其他亞洲地區。該調查亦估計，社會每年因此而導致的經濟損失約達壹百億元（約 70%是僱員在識別及刪除濫發郵件所損失的生產力成本）。

29. 我們可以比較香港與其他地方的濫發電郵問題。根據反濫發電郵軟件公司 Brightmail 統計，濫發郵件於二零零四年五月佔互聯網上全部電郵的 64%，遠高於二零零一年年中的 8%。另一家電郵保安服務公司 MessageLabs 則發現，該公司於二零零四年五月掃瞄的電子郵件當中，有 76%屬於濫發郵件。倘若濫發郵

件的數量一如所料般迅速增加，上述比例將大有可能持續上升。

短訊及多媒體訊息

30. 雖然濫發短訊及多媒體訊息的數量未及使收件匣陷於堵塞的濫發電郵，但過去數年短訊通訊量的上升，毋疑令未經收件人許可而發出的短訊及多媒體訊息有所增加。現時，短訊可以透過互聯網電郵帳戶或固定電話網絡發出。近期的技術和市場發展已大幅減低濫發短訊／多媒體訊息的成本，可能導致濫發郵件數量進一步上升。雖然濫發短訊／多媒體訊息的問題目前比濫發電郵輕微，但如發送短訊／多媒體訊息的成本下降或收費政策改變，則此問題有可能變得嚴重，一如目前日本的情況。

傳真

31. 傳真發件人主要分爲兩類。部分是小型店舖東主，他們使用單一傳真線，促銷本身的產品或服務。他們的經商性質導致有需要列出電話號碼和其他聯絡資料，方便有興趣的客戶聯絡他們。另一類傳真發件人則爲其客戶提供更大規模的直銷服務，當中很多發件人利用大量傳真線，每日二十四小時不停發出傳真廣告。視乎客戶的要求，這些傳真發件人可能任意發出廣告，或只向指定的傳真線用戶發出廣告。

32. 直銷業界會否利用某種電訊服務提供業務，取決於有關服務的收費結構。香港的商業傳真線收費是按月收費，每月低於 130 元。使用傳真線作直銷用途的邊際成本微不足道，香港的直銷業界因而經常使用傳真線作爲傳送方式。

33. 根據本地固網服務營辦商報告，二零零三年內有足夠資料讓固網服務營辦商跟進的投訴數字爲 24 232 宗。在這些投訴個案當中，有 15 491 宗是來自已經把電話號碼登記在「不收傳真名單」的客戶。很多傳真發件人顯然繼續向經已選擇不接收有關訊息的人士發出商業訊息。

34. **政府歡迎有興趣的團體就未經收件人許可而發出的電子訊息的嚴重程度，以及未經收件人許可而發出的電子訊息對他們造成的金錢損失提出意見，並夾附相關紀錄、數據和統計資料。意見書所用的假設，例如有關估計或調查是否根據若干定義作出（如未經收件人許可而發出的訊息或只計算未經收件人許可而發出的商業電郵），亦應清楚列出。**

現行措施及其效用

法例

35. 現行法律架構有若干條文處理有關話音通話的罪行，亦有條文涵蓋濫發郵件的若干部分，但如下述，這些條文並不是用以專門管制濫發郵件的行爲。

36. 在訊息內容方面，例如《淫褻及不雅物品管制條例》（第 390 章）禁止發布或公開展示淫褻及不雅的物品（包括印刷品、錄音、電影、錄影帶、磁碟及電子發布）。《防止兒童色情物品條例》（第 579 章）亦就兒童色情物品的發布作出規定。

37. 然而，香港沒有法例專門就未經收件人許可而發出電子訊息作出規定。

《簡易程序治罪條例》（第 228 章）

38. 《簡易程序治罪條例》第 20 條就與電話、訊息或電報有關的罪行作出規定[1]。該條文曾於一九九一年修訂，當時互聯網主要是限於學術界使用，流動電話使用量尚未高速增長。現行法定條文主要針對無合理因由的滋擾電話，並不旨在處理有關其他電子通訊媒介的垃圾傳真或濫發郵件問題。

《個人資料(私隱)條例》（第 486 章）

39. 《個人資料(私隱)條例》第 34 條就個人資料在直接促銷中的使用作出規定。第 34(2)條將「直接促銷」界定爲

(a) 要約提供貨品、設施或服務；
(b) 就貨品、設施或服務的可予提供而進行廣告宣傳；或
(c) 索求用於慈善、文化、娛樂、政治或其他目的的捐贈或貢獻，

而該等要約、廣告宣傳或索求是藉著以下資訊、貨品或通話進行的—

(i) 藉郵遞、圖文傳真、電子郵件或其他相似的傳訊方法送交予任何人

---

[1] 任何人有以下行爲，可處罰款$1000 及監禁 2 個月—
(a) 使用電報、電話、無線電報或無線電話傳送任何極爲令人厭惡的訊息，或任何不雅、淫褻或威脅性質的訊息；或
(b) 使用上述方法傳送任何其明知是虛假的訊息，旨在對他人造成煩擾或不便，或旨在令他人產生不必要的憂慮；或
(c) 無合理因由及旨在達致任何上述目的而不斷打電話。
(由 1935 年第 36 號第 2 條增補。由 1991 年第 90 號第 28 條修訂)

的資訊或貨品，而該等資訊或貨品是**指名致予某一個或某些特定人士**（粗體字爲本文加上）的；或

(ii) 以特定人士爲對象的電話通話。

40. 《個人資料(私隱)條例》第 34(1)條就直接促銷從業員使用個人資料作直接促銷的目的作出以下規定：

(1) 在首次如此使用該等資料時，他須告知該資料當事人謂如該資料當事人要求該使用者停止如此使用該等資料，該使用者須在不向該當事人收費的情況下照辦；

(2) 如該資料當事人作此要求，該資料使用者須在不向該當事人收費的情況下停止如此使用該等資料。

直接促銷公司作爲資料使用者，在首次使用該等資料進行直接促銷時，應該讓當事人有機會「選擇不接受」(「opt-out」)，以停止接收有關訊息。私隱專員亦已發出電話促銷活動指引[2]。

41. 《個人資料(私隱)條例》的目的，是在個人資料方面保障在世人士的私隱，因而適用於任何直接或間接與一名在世人士（資料當事人）有關的資料，從而可切實用以確定有關人士的身分。《個人資料(私隱)條例》並非旨在處理一般透過傳真或電郵發出的直接促銷訊息，因這些訊息甚少載有收件人的姓名。若無其他可供辨識個人身分的資料，電郵地址本身可能並不構成《個人資料(私隱)條例》所保障的個人資料。

《電訊條例》（第 106 章）

42. 根據《電訊條例》第 27A 條，如濫發電郵涉及藉電訊而在未獲授權下取用電腦（俗稱黑客行爲），即可被處罰。然而，該條文的重點在於未獲授權下取用電腦，而非管制濫發電子郵件的行爲。

《刑事罪行條例》（第 200 章）

43. 《刑事罪行條例》第 60 條規定，*「任何人無合法辯解而摧毀或損壞屬於他人的財產，意圖摧毀或損壞該財產或罔顧該財產是否會被摧毀或損壞，即屬犯罪」*。《刑事罪行條例》第 59 條則規定，就電腦而言，*「摧毀或損壞財產」*，包括*「誤用電腦」*。*「誤用電腦」*指

[2] http://www.pco.org.hk/chinese/publications/fact3_coldcall.html

「(a) 導致電腦並非如其擁有人或其擁有人代表對其所設定的運作方式運作，即使如此誤用不會令該電腦的操作、該電腦內的程式或該電腦內的資料的可靠性減損亦然；

(b) 更改或刪抹電腦內或電腦儲存媒體內的程式或資料；

(c) 在電腦或電腦儲存媒體所收納的內容上增加程式或資料，

而造成導致(a)、(b)或(c)段所提述的任何類別誤用情形的任何作爲，須視爲導致該項誤用情形的作爲」。

44. 例如，倘若濫發電郵者令電腦停止運作，可能已觸犯《刑事罪行條例》第 59 及 60 條。然而，應該留意上述條文旨在懲處導致財產摧毀和損壞的誤用電腦行爲，並非將透過電腦發出未經收件人許可的電子訊息的行爲刑事化。

45. 《刑事罪行條例》（第 200 章）第 161(1)條規定，任何人有下述意圖或目的而取用電腦—

(a) 意圖犯罪；
(b) 不誠實地意圖欺騙；
(c) 目的在於使其本人或他人不誠實地獲益；或
(d) 不誠實地意圖導致他人蒙受損失，

即屬犯罪。意圖犯罪而取用電腦的人士將由於取用電腦行爲而被處罰，並非針對所犯的罪行。該條文的重點亦是取用電腦時的犯罪意圖，而不是管制透過電腦發出未經收件人許可的訊息的行爲。

46. 以上提及的現行立法條文均並非直接管制濫發郵件的問題。

自願性的工作守則

電郵

47. 香港互聯網供應商協會於二零零零年二月發出反濫發電郵工作守則，包括未經收件人事先要求或許可而大量發出的電郵訊息或透過電郵發出的物品。該守則列明對被發現從事濫發郵件行爲的人士的罰則，例如暫停服務。然而，該守則屬自願性質，濫發郵件者亦並非該協會的成員。

48. 此外，該守則建議互聯網服務供應商應就減低濫發郵件可能性採取預防措施，包括：

(1) 禁止轉發電郵；
(2) 限制互聯網電郵及預繳帳戶的外發電郵量；
(3) 限制接駁埠 25 的使用；
(4) 互聯網服務供應商應印製處理濫發電郵程序的印行本或將該文本放置在網頁上。該指引應包括設立「濫發電郵」戶口，接收及跟進客戶有關濫發電郵的投訴。

49. 香港互聯網供應商協會於二零零一年六月就該指引的效用進行調查，發現雖然該指引有助減少濫發電郵，但由於互聯網的發展、自動濫發電郵軟件及互聯網在中國內地的迅速普及等因素，以致效果不彰。

50. 香港互聯網供應商協會發現，會員供應商採用由http://mail-abuse.org運作的 Real-Time Blackhole List (RBL)，有助減少濫發電郵。然而，RBL 在美國運作，未能協助香港的互聯網服務供應商辨識來自中國內地或中華台北的濫發電郵。故此，香港互聯網供應商協會建議制訂被合理地懷疑爲傳送濫發電郵的本地電郵伺服器清單(M-List)。互聯網服務供應商其後便可以透過修改電郵伺服器的設定，查核來自 M-List 伺服器的電子郵件，並作出特別處理。特別處理包括掃瞄病毒、加上標籤以供電郵收件人辨識或將郵件退回發件人。香港互聯網供應商協會進一步建議，M-List 應由一個中立機構運作和維持，例如香港電腦保安事故協調中心(HKCERT)。

51. 電訊局曾接獲投訴，指濫發電郵者在未經收件人許可的情況下發出廣告時，僞冒成有關客戶的互聯網服務供應商的網主。客戶被標頭誤導，以爲郵件是由服務供應商的網主發出，因而閱讀這些郵件，最終發現只屬未經許可而發出的郵件。感到不滿的客戶往往向互聯網服務供應商發出投訴電郵，怪責服務供應商濫發電郵。互聯網服務供應商認爲，這不但會擾亂網絡營運，亦會嚴重損害他們的商譽。

52. 根據有關檢討，香港互聯網供應商協會認爲，現行自願性質的架構未夠全面，不足以處理所有有關未經收件人許可而發出的電郵的問題，並建議引入懲罰性條文，以立法方式解決此問題。

短訊服務及多媒體訊息服務

53. 香港六家流動電話營辦商於二零零一年十二月就「處理擅自發出的宣傳性跨網短訊」的工作守則達成協議，當中規定營辦商發出宣傳性跨網短訊的指引。然

而，該守則屬自願性質，並不包括未經收件人許可而發出的網內短訊，亦不禁止營辦商向本身的客戶發出未經許可的訊息。

傳真

54. 根據現時的行政架構，不欲收到未經許可而發出的傳真廣告的傳真線用戶可申請將傳真號碼納入「不收傳真名單」，所有傳真廣告的發件人均須遵從。收到未經許可而發出的傳真廣告的人士可向其固網服務營辦商提出投訴。若投訴成立，有關發件人將被制裁，包括暫停或終止其傳真線服務。

55. 傳真廣告的發件人須遵從由電訊局發出的自願性質的指引，當中界定透過傳真發出廣告的可接受安排。有關安排包括：

(1) 不應向「不收傳真名單」上的號碼發送未經收件人許可的廣告；及

(2) 廣告應載有識別發件人所需的資料和聯絡方法，讓收到傳真訊息的人士能夠聯絡發件人，以便行使不再接收該等傳真廣告的權利。

56. 本地有線固網服務網絡營辦商已制訂工作守則，規定處理有關未經收件人許可而發出的傳真廣告的投訴的標準程序。電訊局於二零零四年一月二日修訂上述自願性質的工作守則。該守則第 6 段清楚列明，雖然該守則屬自願執行性質，固網服務營辦商仍有責任保障電訊服務使用人的利益，以及告知他們以正確和令人接受的發送傳真手法來達到廣告宣傳的目的。電訊管理局局長（電訊局長）認爲，固網服務營辦商應提供以上良好的客戶服務。新指引亦訂定更嚴厲的罰則，容許固網服務營辦商在收到三宗成立的投訴，即可截斷指定地址的登記客戶的所有線路，而不止是被投訴的線路。

技術工具

57. 現時，市面上有一些技術工具可減少未經收件人許可的電子訊息的數量；例如，電郵方面的軟件工具可在幾個層面局部解決濫發電郵的問題。很多控制濫發電郵的工具可供最終用戶選擇，而且多是免費提供，而互聯網服務供應商可用其他阻截方法。以下是一些常用技術工具的例子。

58. 然而，互聯網服務供應商過濾訊息須付出時間和金錢，而這亦會減慢網絡效能，且不能減少由來源發出濫發訊息的數目。另一個問題是，若要過濾產品能阻截大部分濫發訊息，同時又不會過濾有用的訊息，那是不易設計、配置或安裝的。

用戶的安排

59. 在中短期，技術工具和加強消費者意識的方案或可緩和濫發訊息的問題。

60. 傳真用戶 (就垃圾傳真而言) 、互聯網用戶 (就濫發電郵而言) 和流動電話用戶 (就濫發短訊及多媒體訊息而言) 可不理會和刪除濫發訊息。用戶應依照個別網絡營辦商發出的用戶指引，亦建議互聯網用戶避免到濫發電郵者製造郵址名單的地方，如新聞組、聊天室和公共通訊錄。

61. 若互聯網用戶定期在網上登出地址，建議專爲這些郵件開設一個專用電郵戶口，而個人電郵戶口則只向家人和朋友披露。此外，他們可透過加字或額外符號變更電郵地址，再向他們的朋友加以解釋如何獲取正確地址，這樣便能確保自動電郵掃描器收集的電郵地址不能運作。

阻截裝置

62. 這些工具嘗試根據電郵訊息內容和標頭阻截濫發電郵。這些工具可學習根據用戶對收到電郵的分類分辨濫發電郵。

63. 「許可名單」 (whitelist) 就是被證實爲正當發送人的電郵地址名單。在這系統下，伺服器將會儲存所有未能辨別地址的電郵，同時自動向電郵發送人發出訊息。自動發出的訊息會要求對方回覆電郵或到網站輸入資料，從而核實發送人確有其人，而不是自動發送大量電郵的程式。

64. 這些工具讓商業機構和個人只接收由認可來源發出的電郵，或與過濾工具一併使用。這個方法或適用於部分家居用戶，但對商業機構、政府部門和經常收到不認識的人所寄電郵的個別人士並無效用。

65. 數家機構亦已提供濫發電郵黑名單，收集已知濫發電郵者的 IP 地址的資料。這些名單可納入在過濾工具內，以阻截所有來自黑名單的電郵。然而，因爲 IP 地址並非總是用於同一特定的電腦或用戶，這個方法的弊處就是可能阻截非濫發的電郵。阻截由特定 IP 地址發出的電郵，可能阻截所有使用同一互聯網服務供應商的用戶的電郵。

66. 就傳真而言，大部分垃圾傳真發送人在發送垃圾傳真時，會啓動來電號碼顯示中的停止示號功能 (即發送人的電話號碼不會顯示在接收一方的來電顯示中)。除了於發送一方實行措施，接收一方也可做些預防措施。有些客戶不希望收到停止示號的垃圾傳真，所以部分固定網絡服務營辦商向他們提供名爲「拒接停示者」的篩選服務。不過，當透過專用自動電話交換系統發送，而來電號碼通

常顯示爲 「O」 或「離區」，這項措施便不能阻截這類垃圾傳真。

互聯網服務供應商的努力

67. 互聯網服務供應商一直在互聯網伺服器和網絡實行技術措施，如阻截其網絡的外送傳輸服務協議 25 埠 (簡單郵件傳送協議) 的所有封包及關閉電郵伺服器的轉送功能。這樣能確保濫發電郵者不能利用撥號服務，接駁至其互聯網服務供應商的開放式電郵伺服器。這亦可防止客戶不慎操作開放式電郵伺服器，在不知情的情況下被其他地方使用濫發電郵。互聯網服務供應商亦提供客戶指引和適當的措施以打擊濫發電郵，例如向客戶提供適用於電腦的過濾軟件。

可行的解決辦法

業界合作

68. 現時，業界已就透過傳真、電郵和短訊服務發放未經收件人許可的訊息的行爲訂定自願工作守則。由於這些守則屬自願性質，因此業界營辦商 – 固定電訊網絡服務營辦商、互聯網服務供應商和流動電話營辦商嚴格遵守這些守則，協助打擊濫發郵件所造成的問題便非常重要。

69. 鼓勵業界組織例如香港互聯網供應商協會及其全體成員：

- 以香港互聯網供應商協會的工作爲基礎，實施有關實務守則以對付濫發電郵；
- 向互聯網服務供應商 (及其客戶) 提供更清晰的實用指引，以對付濫發電郵；
- 進一步制定策略使互聯網用戶關閉開放式轉送郵件伺服器；及
- 爲其客戶印製處理濫發電郵的指引。

70. 業界營辦商亦可團結一致，編製一份公用的濫發電郵者黑名單。這樣能大大改善現行不受監管的黑名單。現行的黑名單並不奏效，很多時會使無辜的互聯網用戶受害，當中很多更曾被違規的濫發電郵者愚弄。

71. **政府現就應否推行上述第 68 至 70 段中提出業界合作的建議徵詢意見，包括這些措施應否屬自願性質，以及是否有任何部分應改爲強制性。**

用戶教育

72. 香港電腦學會資訊保安專家小組提交名爲*「反濫發電郵建議：適當的立法」*(http://www.hkcs.org.hk/en_hk/doc_general/as-recommend-final.pdf) 的文件中表示，只採用單一方法不能有效打擊濫發電郵。相反，應結合立法、教育和技術控制以達致最大效益。在澳洲，澳洲網際網絡產業協會視教育爲其反濫發電郵運動的重要一環，並以「別試 – 別買 – 別回應」爲口號。

73. 在經濟合作及發展組織(經合組織)濫發電郵研討會背景文件中，經合組織承認立法只能有限度地保護用戶預防海外濫發電郵者。但是，若由精明的用戶採取行動，則不論濫發電郵者身在何處，也會有所幫助。澳洲國家資訊經濟辦公室在編寫的濫發電郵回顧報告提出，消費者教育是反濫發電郵策略中的關鍵因素，特別是教育和授權消費者，使他們：

- 能精明選擇有關減少濫發電郵的策略和技術；

- 更清楚明白購買由濫發電郵推廣的產品的陷阱，包括因大部分產品不可靠的性質而產生的風險，以及購買行爲如何提高濫發電郵的商業價值；

- 更清楚明白如何在網上保護他們的私人資料，如電郵地址，從而使濫發電郵變得困難；

- 更清楚明白他們在所有關於濫發電郵和可用的補救方法所享有的權利。

74. 相關業界組織，如香港互聯網供應商協會、香港反濫發電郵聯盟、香港電腦學會和 ADMA 可以合作推廣有關濫發電郵的資訊，以引起消費者的關注及向消費者提供準確資料和實用對策。

75. **政府現就應否由業界推行這類反濫發電郵運動徵詢意見，及如應該的話，運動應採取的形式和包含的宣傳訊息。**

技術解決方法

76. 在濫發電郵方面，市面上有反濫發電郵的解決方法，如使用「黑名單」、「許可名單」(「經核實發送人名單」) 的過濾器及數碼簽名計劃等，以過濾未經收件人許可的電郵，從而保障和幫助商業用戶、互聯網服務供應商和個人用戶。大部分反濫發電郵解決方法均結合多個技術項目。無論是個別公司，還是多間公司

共同合作，都曾嘗試尋找技術解決方法以防止/減少濫發電郵；例如，在二零零三年四月，微軟、AOL、Earthlink 和雅虎宣布合作阻截不明訊息及阻止濫發電郵者登記虛假電郵戶口。最近，微軟估計由公司專家組成的反濫發電郵技術及策略小組，將結合所有反濫發電郵策略和研究及發展的成果，在兩年內提供技術方法，解決濫發電郵問題。此外，一些互聯網服務供應商亦合作尋找濫發電郵的技術解決方法。

77. 在傳真方面，客戶可申請使用由部分固定網絡服務營辦商提供的「拒接停示者」服務，以避免收到任何匿名電話，包括沒有來電號碼顯示的垃圾傳真電話。

78. **政府希望就現有的技術解決方法和其效用徵詢意見。**

立法

79. 部分司法管轄區，如美國、英國和澳洲，已引入特定的反濫發電郵法例，惟仍有其他地區未有採納。**附件**提供有關海外主要司法管轄區反濫發電郵法例的詳細資料，資料來源爲*經合組織濫發電郵研討會背景文件* (*參考* DSTI/ICCP (2003) 10/FINAL)。

80. 許多業界組織要求制定綜合法例，處理透過電子媒界發放各種形式的未經收件人許可的訊息。香港反濫發電郵聯盟提出的*「立法：打擊濫發電郵重要支柱之一」*(http://www.hkispa.org.hk/spam/20040113-coalition-paper.pdf)白皮書中，指出對付濫發電郵問題全面及有效的解決方法中，特別針對濫發電郵的法例佔重要一環，並促請政府就有關打擊濫發電郵草擬特定法例展開公眾諮詢。香港電腦學會的資訊保安專家小組亦建議應頒布新法例特別處理濫發電郵。

81. 然而，有人認爲立法將爲各界帶來額外符合規定的成本和責任。很多真正的商戶均透過電郵、電話或傳真進行促銷活動，當中負責任者佔大多數。有人認爲，新法例的制定將爲這些商戶帶來額外的責任和成本。此外，政府留意到發放未經收件人許可的訊息（尤以電郵和傳真爲然），是中小型企業廣爲採用的既有效又低成本的推廣方法。有意見指出，對未經收件人許可而發出的電子訊息強加額外規定，可能妨礙中小型企業使用上述推廣方法；亦有人認爲，就未經收件人許可而發出的電子訊息制定新法例，會影響直銷商戶。這些商戶將需要檢討，甚至重新制訂直銷策略，以符合相關法例。他們可能選擇修改或重新編纂只包括符合準則人士的名單，或會檢討業務模式，因而帶來額外的成本。其他人或會關注到反濫發電郵新法例賦予執法機關的新權力，可能侵犯個人在個人通訊例如電郵、傳真、短訊及多媒體訊息方面的私隱。

82. 反濫發電郵新法例的效用主要取決於執法的效果及施加的懲罰性質(即民事

及／或刑事）。執行反濫發電郵法例時可能出現多種困難：

(1) 當局難以追蹤濫發電郵者。他們以多種方法隱藏身分，寄件地址往往以隨機方式安排，因而難以辨識。濫發電郵軟件程式亦可自動產生錯誤的標頭和回覆地址資料。錯誤的標頭令濫發電郵者得以迴避收件人從電郵名單刪除名稱的要求，亦令人無法追查他們的身分。其他濫發電郵者則透過互聯網在其他國家找尋匿名轉發，令訊息難以追蹤。部分濫發電郵者會登記免費電郵帳戶，並於被揭發前棄置。他們亦會使用有多個帳戶的程式，當其中一個帳戶被終止後，便會立即登入另一個帳戶。濫發電郵者還會「僞造」地址，在發件人名稱使用錯誤的資料，包括錯誤的資訊或使用與濫發電郵無關的商業機構名稱。

(2) 濫發郵件的跨境性質亦增加了執行反濫發電郵法例的難度。濫發電郵無分國界，根據香港互聯網供應商協會在二零零三年十二月進行的濫發電郵調查顯示，只有 5%的濫發電郵是來自香港，其餘 95%均是來自海外。將法例賦予的司法管轄權延伸至海外的濫發電郵者並不容易。即使能夠做到，執法機關在境外執行法例時亦可能遇上困難，例如跨境搜集證據。

(3) 執法資源及執法優先次序亦可能構成問題。反濫發電郵法例的執法性質屬於資源密集。由於可能缺乏資源以及其他工作較爲迫切的關係，不少海外司法管轄區的檢控機關均未有優先處理濫發電郵的檢控工作。美國有大部分濫發電郵訴訟均由私人提出，可見即使通過新的聯邦法例，執法工作將繼續構成嚴重問題。即使是資金最豐厚和最有魄力的原告人，雖然經已贏得多宗官司，但亦面對日益增加的濫發郵件。濫發電郵問題持續的原因往往不是欠缺法例，而是執法資源相對缺乏。

(4) 反濫發電郵法例的懲罰性質亦會影響其效用。美國的《CAN-SPAM 法》制定民事和刑事罰則，令聯邦貿易委員會、司法部長及互聯網服務供應商得以控告違反法例的公司：聯邦貿易委員會的檢控一旦成立，初犯者可被判入獄三年，由電子郵件所得的收入以及犯案期間所用的任何電腦、軟件、技術或設備均會被沒收。另一方面，司法部長可循民事訴訟執行《CAN-SPAM 法》，就每個訊息徵收罰款 250 美元，最高可達 200 萬美元。互聯網服務供應商亦可執行《CAN-SPAM 法》，循民事訴訟申索實際的金錢損失。澳洲《濫發電郵法》選擇民事而非刑事罰則，是經過深思熟慮的決定，有關理由如下：

(a) 民事訴訟的舉證標準較低（即衡量相對可能性而不是無合理疑點）；

(b) 處理證據方面的限制可能較寬鬆(國內及不同司法管轄區之間轉交投訴亦然)；

(c) 民事訴訟所施加的罰款一般較重；

(d) 根據法律政策的觀點，民事罰則與罪行的嚴重程度比較相稱；

(e) 民事罰則制度較具彈性及能夠提供不同的罰則(包括警告、違例通知及法庭訴訟)；

(f) 行政成本較低。

83. 海外司法管轄區的立法措施相對較新，效用仍然有待觀察和試驗。有人建議，香港可加強現有對付濫發電郵的措施，而不應即時制定有關法例。當海外司法管轄區累積更多反濫發電郵法例執法經驗後，香港將可根據海外經驗評估應否制定類似法例。**政府希望就立法打擊濫發電郵的利弊徵詢意見，以及應否加強現有對付濫發電郵問題的措施和如應該的話，如何加強有關措施。**

84. 如選擇立法，政府需要就上述第 5 至 14 段的定義問題，諮詢公眾意見。政府知道發放未經收件人許可的電子訊息，是商業機構 (特別是中小型企業) 既有效又低成本的推廣方法，而對濫發電子訊息引入額外規定，必會爲擬發放未經收件人許可的電子訊息作推廣用途的人，帶來額外的成本。政府在考慮是否引入新法例及其內容時，一方面應顧及對未經收件人許可的電子訊息的寄件者的影響，而另一方面應顧及對未經收件人許可的電子訊息的收件人，以及其他有關團體如互聯網服務供應商帶來的成本／滋擾。

85. 如選擇立法，將有多項問題需要細心考慮，當中包括：

(1) 法例的範圍爲何？是否應該採用涵蓋所有透過電子形式發出而未經收件人許可的訊息的技術中立方法，或應該只涵蓋有大量投訴的電郵和傳真？

(2) 法例應否只包括「商業」電子訊息或應否同時包括「非商業」電子訊息？

濫發電郵的特點是有商業目的：推銷或銷售產品或服務。然而，部分收件人可能會視一些非商業訊息爲濫發電郵，如有關政治題材或宗教目的而未經收件人許可的大量訊息，又或是附有病毒的大量訊息。倘若建議的法例包括非商業訊息，可能與言論自由和宗教自由等原則互相抵觸，

亦會增加執法難度和相應的支出。

(3) 法例應否包括「大量」的概念？若包括在內，應採用甚麼形式？

如果任何建議的法例包括「大量」的概念，主要論點會是如何界定在某時段內發放某數量的訊息可視爲大量傳送。另一種方法是不採用「大量」的概念，而是根據發送訊息的數量訂明不同罰則。

(4) 促銷電話、話音或錄像是否不應納入電子訊息的定義？

由於從業員投放於電話促銷的資源遠多於其他電子訊息，電話促銷活動的問題一般相比並不嚴重。所以，新法例或不需要包括話音或視象通話。

(5) 應否使用事先經過許可的模式禁止未經收件人許可的電子商業訊息？若選用，應採用甚麼形式，例如從已存在的商業關係得到的明示或默示？

方案一是任何新法例應規定除非事先取得同意（明示或暗示），否則任何人也不能發放有商業目的的未經收件人許可的訊息。另一個方案就是如普通郵件一樣，不需要事先取得同意。

(6) 應否採用「選擇接受」（「opt-in」）／「選擇不接受」（「opt-out」）的方案？

「選擇接受」是指未經收件人許可訊息的寄件者需要在發出任何訊息之前，向預期的收件人事先取得明示或暗示的同意。「選擇不接受」要求未經收件人許可訊息的寄件者需要向收件人提供方法，通知寄件者不希望再收到其他未經收件人許可的訊息。在已立法對付未經收件人許可而發出的電子訊息的經濟體系當中，歐盟國家及澳洲採用「選擇接受」的方式，而美國、日本和南韓則採用「選擇不接受」。

(7) 任何建議的法例是否應就電郵標頭的標籤制定一些強制的要求，如需要，應有甚麼要求?

爲對付濫發電郵者在訊息標頭使用不實資訊的問題，任何建議的法例可要求商業電子訊息正確地識別和標籤。具體規定有待仔細研究。

(8) 建議的立法應否包括對收集電郵地址、自動產生或共享名單的限制？如

需要，應作出甚麼限制？

很多濫發電郵者用 webcrawlers 網站搜尋器搜尋互聯網，收集所有找到的電郵地址。其他濫發電郵者從網站，如新聞組、聊天室和公共通訊錄，製造郵址名單。有些利用自動方法產生電郵地址。有人提議禁止從網站收集電郵地址，和禁止使用自動方法產生電郵地址。其他提議法例應禁止互聯網供應商之間買賣郵址名單。

(9) 有關執法機構應獲賦予的調查和執法權力範圍爲何？網絡／服務營辦商在向執法機構披露資料、終止或刪除濫發電郵方面有何權利和責任？

若要任何建議的法例有效，有關執法機關必須有法定調查及執行的權力。例如，執法機關應獲賦予法定權力追查濫發郵件的來源。此外，根據現行的自願體制，固網服務營辦商和互聯網服務供應商因憂慮可能洩露機密和侵犯私隱，或會不願意公開濫發電郵者的身份。這引起一個問題，當懷疑電話及／或其他電子通訊媒界濫發郵件時，應否規定網絡和服務供應商公開其來源。固網服務營辦商和互聯網服務供應商有時需要終止或刪除濫發電郵。這亦引起一個問題，就是在確保通訊自由流通的情況下，固網服務營辦商和互聯網服務供應商是否可以終止或刪除濫發電郵。

(10) 因推出有關濫發電郵的額外措施而導致因符合有關規定的成本增加的本質及幅度爲何？

引入管制濫發電郵的措施，難以避免爲想發放未經收件人許可的訊息作促銷用途的人帶來額外成本。成本多少則視乎不同因素而定，其中包括規管類型 (如「選擇接受」或「選擇不接受」)。故此，當局制訂立法時，問題在於建議的法例所導致的成本的類別和幅度。

國際合作

86. 濫發電郵是全球的問題。制定對內措施處理問題，只能減輕來自香港的濫發電郵問題。香港互聯網供應商協會在二零零三年十二月所進行的研究顯示，香港的濫發電郵中有 5%來自香港，另外 20 至 40%來自其他亞洲地區，其餘來自其他地方。源自香港的濫發電郵亦可能對其他地方的用戶造成問題。若這是實況，香港的反濫發電郵法只能協助紓緩部分問題。我們需要依賴國際合作措施處理大部分來自香港境外的濫發電郵。

87. 在多邊層面上，香港應與經濟合作及發展組織 (經合組織)、亞太經合組織或

其他有關組織發展國際合作機制處理濫發電郵問題。

經濟合作及發展組織（經合組織）

88. 在二零零零年，經合組織發出電子商務保護消費者指引。以下的原則有關濫發電郵問題：

(1) 商界不應利用電子商貿的特色，隱藏其真正身份和位置，或避免遵守保護消費者的標準和／或執行機制。

(2) 應清楚表明是廣告和促銷。

(3) 商界應發展和推行有效易用的程序，供消費者選擇是否希望收到未經收件人許可的商業電郵訊息。

(4) 如消費者已表示不希望收到未經收件人許可的商業電郵訊息，須尊重其選擇。

89. 二零零三年六月，經合組織採用*經合組織保護消費者免受跨境欺詐和詐騙商業活動指引*，這新指引鼓勵國際合作對付跨境欺詐和詐騙。含有詐騙或欺詐內容的濫發訊息或會包括在指引的範圍，這爲將來實行指引中提及的合作執法架構定下基礎。

90. 二零零四年二月二日至三日，經合組織舉辦一個濫發電郵工作坊，其中一個目的是討論以後採取的行動，希望能加強國際間的合作，處理濫發電郵問題。經合組織濫發電郵工作坊的背景文件可參考以下網頁：
http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF

亞太經濟合作組織（亞太經合組織）

91. 在二零零三年亞太經合組織部長級會議上，部長贊成就未來進行有關「濫發電郵」的工作，與經合組織緊密合作。亞太經合組織的電子商貿督導小組贊成處理濫發訊息的工作計劃，並提出需要研究幾個重要議題，當中包括：

(1) 識別和報告因各種形式的濫發電郵及郵件所引起的損害；

(2) 識別和鼓勵現有跨境合作方法，打擊欺詐和詐騙的濫發訊息；

(3) 識別和報告結合本地政策或法律及其他解決方法，可協助預防因濫發郵件所引起的損害，並作出反應；及

(4) 使用可計算的標準評估打擊濫發郵件措施是否有效。

92. 香港特區是亞太經合組織的成員，因此會繼續積極參與以上各項工作。

世界資訊社會高峰會

93. 在二零零三年十二月十二日世界資訊社會高峰會發表的*原則聲明*中，國際電聯成員國清楚表明建立一個包容的資訊社會，是建立信心和安全地使用資訊和通訊科技的重要原則。在聲明的第 37 段，成員國清楚表明，「*無論是對用戶、網絡，還是整個互聯網，濫發郵件是一個重要且日益嚴重的問題，應在適當的國家和國際層面上處理濫發郵件和網上安全的問題。*」在世界資訊社會高峰會採用的*行動方案*中，成員國進一步同意在國家和國際層面上，應採取適當打擊濫發郵件的行動。

徵詢意見

94. 政府現就第 34、71、75、78 及 83 段徵詢意見。任何就本諮詢文件提出的意見須於二零零四年十月廿五日或以前送達電訊管理局。任何人提交意見時須注意，政府可能會公開接獲的所有或部分意見，並會以認爲合適的方式披露提出意見的人士的身份。意見書內屬商業秘密的部分必須清楚註明。政府在決定是否披露有關資料時，會考慮這些標記。政府會視乎回應決定下一步的行動，包括就有關問題進行第二輪諮詢。意見書應送交：

香港灣仔
皇后大道東 213 號
胡忠大廈 29 樓
電訊管理局
經辦人：公共事務經理（消費者及綜合事務）

電子版的意見書應電郵至 uem-consultation@ofta.gov.hk。意見亦可傳真至 2803 5112。

電訊管理局
二零零四年六月廿五日

附件　海外部分司法管轄區的反濫發電郵措施

澳洲

在二零零三年十二月二日，澳洲國會通過《二零零三年濫發電郵法》。該法例對商業電子訊息採取「選擇接受」制度。電子訊息包括電郵、即時傳訊、傳送到流動電話的文字或視象訊息及在規例中定義的訊息。該法例亦要求有關收件人地址準確及取消選用的功能運行正常。該法例禁止分發及使用收集電郵地址工具或已收集的地址清單，並鼓勵訂立適當的業界守則。該法例包括一套靈活變通的民事制裁制度，例如警告、違例通告和賠償懲罰。違反法例的濫發電郵者每日罰款最高可達 44,000 澳元，而違例的組織則可每日被罰最高 22 萬澳元。該法例亦禁止使用收集名稱和攻擊代碼名以進行濫發電郵或相關活動。澳洲通訊局(ACA)將有權調查、發出違例通告和提出訴訟。若任何人或公司因濫發電郵者的活動蒙受損失或傷害，澳洲通訊局可代其向法庭申請賠償。

加拿大

在制定《個人資料保護及電子文件法》之前，加拿大政府認爲發放未經收件人許可的推廣及產品資料 (印刷或電子模式)並非違法，而加拿大也沒法例規管[1]。不過，當上述法例在二零零一年一月生效後，電郵地址被視爲個人資料，所以亦受該法例條文限制。未經資料當事人同意而收集及使用其個人資料(例如電郵地址)，會違反該法例的規定。加拿大私隱專員負責執行該法例。

該法例亦規定儲存電郵地址的機構及其他有關方面，爲個人資料提供適當的保安措施。該法例通過後的首三年，法例適用於由聯邦規管的企業，以及從事個人資料的跨省和國際買賣的私人公司。此後，所有使用個人資料作商業活動用途的組織都包括在內。因此，購買、售賣、租借或交換電郵地址名單 (即發送大量未經收件人許可電郵的依據) 的公司若在省內或國內進行有關交易，即受制於該法例的條文[2]。不過，現時沒有對濫發電郵訂定具體的規定。

雖然加拿大沒有具體處理濫電郵的法例，但若濫發電郵傳播誤導訊息或涉及欺騙性的推廣行爲，可能會違反競爭法的規定及由加拿大競爭局執行的其他法令。

---

[1] 參閱加拿大工業部（一九九九年），「互聯網及未經收件人許可而大量發出的電子郵件政策」，七月，http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html，二零零四年一月九日。

[2] 參閱加拿大工業部（一九九九年），「互聯網及未經收件人許可而大量發出的電子郵件政策」，七月，http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html，二零零四年一月九日。

歐洲聯盟

在二零零二年七月十二日，歐洲議會和歐洲理事會就電子通訊界處理個人資料及保護私隱發出新指引 2002/58/EC。歐盟就商業電郵通訊（包括短訊服務）採用「選擇接受」方法。之前，「選擇接受」方法適用於傳真及自動撥號機。

在新指引下，「電子郵件」的範圍很廣闊及屬於技術中立，包括所有毋須發件人及收件人同時參與的電子通訊方式，即傳統的「電郵」，以及短訊服務和多媒體訊息服務等。新指引提出三項有關未經收件人許可而發出的電子通訊的基本原則。首先，根據第 13(1)條，除非事先獲有關人士同意，否則成員國須禁止透過傳真、電郵或短訊服務及多媒體訊息服務等其他電子傳訊系統發送未經收件人許可的商業通訊（選擇接受）。這項制度適用於發給個人（自然人）的商業通訊，但成員國可將通訊範圍延伸至商業機構。選擇接受的制度有限度地豁免使用現有客戶在銷售時提供的聯絡資料（第 13(2)條），但只可以由同一名合法人士用於促銷「類似」產品或服務，而客戶在資料收集及其後每次收到訊息時均獲明確指示可以「選擇不接受」。第二，指引禁止偽冒發件人的身分。第三，直接促銷訊息必須包括有效的回郵地址，以便收件人容易地免費「選擇不接受」訊息。

新指引列明，爲執行法例，成員國可引入儲存通訊量及單元數據的條文。新指引亦進一步引入控制網頁的「cookies」。「cookies」和類似的追蹤裝置受新的開放規定所限 – 任何使用這類裝置的人士必須提供有關資料，而訂戶或用戶可拒絕接受這些裝置。

日本

在二零零二年七月，兩條管制濫發電郵的法例正式生效。其中一條是《管制指定電子郵件傳送法例》(2002 年第 26 號法例)，目的是管制未經收人許可的商業電郵的傳送。法例強制未經收件人許可電郵的發送人顯示發送人的姓名、聯絡資料，及若電郵是廣告，在標頭開始標明沒有同意或要求收到電郵，從而使客戶可選擇自動攔截所有含有未經收件人許可的廣告郵件。法例亦禁止傳送電郵至隨機產生的電郵地址。此外，法例亦防止發送人向透過電話或電郵通知發送人不欲收到電郵的收件人發送電郵。總務大臣發布行政指令強制非法發送人遵守法例。若發送人在收到指令後違反法例，會被罰款 50 萬日元 (4,180 美元)。若造成系統問題，法例批准電訊傳送者可拒絕濫發電郵者的電郵。自從法例在二零零二年七月生效後，總務大臣已發布幾個行政指令。

另一法例是一項修訂，更新《1976 年指定商業交易法例》(2002 年第 28 號法例)，這條法例管制郵購銷售，而制訂的目的是保護消費者避免剝削的推廣手法，如直接促銷。法例向用戶提供「選擇不接受」的選擇，規定未經收件人許

可電郵的發送人顯示發送人的姓名、聯絡資料，及若廣告以電郵形式發放，在標頭開始標明沒有同意或要求收到電郵，從而使客戶可選擇自動攔截所有未經收件人許可的廣告郵件。法例亦要求發送人在電郵中通知收件人如何拒絕接收廣告。廣告一經收件人拒絕，產品售賣商或服務供應商即禁止再發送廣告。日本關稅局向可能違法的產品售賣商或服務供應商發出警告訊息 (二零零二年發出 3700 個訊息)。若他們不遵守警告訊息，日本關稅局會向他們施加政府指令 (在二零零三年十月兩間公司收到這類指令)。違反此條新法例最高可被判監禁兩年或罰款 300 萬日元 (24,000 美元)。[3]

韓國

《推廣資訊、通訊、通訊網絡使用及資訊保護法》禁止向明確表達意願的收件人傳送商業廣告等濫發電郵。法例亦禁止透過技術操縱，漠視「選擇不接受」的要求。法例禁止透過電郵、電話、傳真或其他途徑向青少年發送成人廣告。法例亦規定發送人清楚明確指出傳送的目的和其中的主要內容，以及發送人的姓名、聯絡方法及是否「選擇不接受」。法例規定在標頭標示“ADV”或“ADLT”，及提供清楚顯示收件人拒絕收取訊息或廣告的方法。發送人不准在標頭使用違規的標籤。

此外，禁止透過使用程式或技術方法收集電郵地址以濫發電郵，亦禁止分享、售賣、交換或向其他人提供在網絡布告板收集到的電郵地址清單。此外，法例亦指出，如互聯網服務供應商擔心大量湧入的濫發郵件會造成嚴重阻塞，可拒絕提供傳送資料的服務。現時，韓國採用「選擇不接受」的模式，然而，在二零零三年十月十九日，韓國資訊部（MIC）宣布將會在流動電話服務引入「選擇接受」模式。由於修改現行法例需時，首先會透過流動服務供應商與資訊服務供應商之間的使用協議實行「選擇接受」的模式。這些協議會在二零零三年年底前實行。資訊通訊部亦禁止在部分時間發送所有廣告訊息，例如由晚上九時至早上八時。資訊通訊部擬在二零零四年年初修改有關法例。

新西蘭

雖然新西蘭現時未有濫發電郵法例，但正積極考慮立法的建議。

斯洛伐克共和國 – 沒有法例

斯洛伐克共和國現時沒有有關濫發電郵的法例。

---

[3] 參閱Cramer, Evan(二零零二年)，「未來的無線濫發郵件」，*Duke Law and Technology Review*, Rev. 0021，www.law.duke.edu/journals/dltr/articles/2002dltr0021.html，二零零四年一月九日。

土耳其

現時沒有法例針對濫發電郵。不過，電腦系統管理員和互聯網服務供應商工程師一直都有進行討論，並進行一些試驗工作開發解決方法，以減低濫發電郵對互聯網通訊的負面影響。

英國

由於電郵地址包括個人姓名，所以被視爲個人資料，因此必須根據《1998年資料保護法》的規定處理。這表示若任何公司在個人要求停止收取濫發電郵後，仍繼續處理包括個人資料的電郵地址，以發放未經收件人許可的推廣通訊，即違反法例清楚列明的處理規定。

在二零零三年三月，英國貿易及工業部引入新的反濫發電郵法例，包括「選擇接受」規定。法例在二零零三年九月獲通過，並在二零零三年十二月十一日生效。根據新法例，公司在推廣前，必須得到電郵收件人的明確批准。法例准許個人控告公司透過發放未經收件人許可的電郵進行的推廣。法例亦規定網頁向消費者提供選擇，在放「cookies」在其電腦之前，可選擇拒絕，以及禁止所有未經收件人許可的文本訊息。資訊署長有更大權力去跟進投訴。在新法例下的「選擇接受」規定並不適用於公司電郵地址，即法例的「選擇接受」規定不包括大部分工作地址。

美國

在二零零三年十二月十六日，美國通過濫發電郵的法例（《CAN-SPAM法》），在二零零四年一月一日對濫發電郵採用「選擇不接受」模式。法例禁止使用錯誤或誤導的標題、標頭資料及欺騙性的標題。法例規定未經收件人許可的商業電郵發送人提供「選擇不接受」的機制，及依從收件人「選擇不接受」的要求。法例規定須清楚明確地顯示該訊息是廣告。發送人必須在電郵中提供正確的郵遞地址，及有效的電郵地址。法例亦禁止收集電郵地址、攻擊代碼名及僞裝。法例亦訂下新的刑事罪，例如，法例將故意使用僞造的標頭發放未經收件人許可的商業電郵定爲刑事罪。最後，法例規定聯邦貿易委員會 (FTC) 制訂計劃及時間表，以推行「不要電郵」資料系統，並在法例生效起六個月內，向國會報告任何有關資料系統的關注。

＊ ＊ ＊