出國報告（出國類別：參加國際會議）

出席第十一屆倫敦行動計畫
(LAP；London Action Plan)
年度會議報告

服務機關：國家通訊傳播委員會
姓名職稱：蘇勇吉科長
派赴國家：愛爾蘭（都伯林市）
出國期間：2015 年 6 月 6 日至 6 月 12 日
報告日期：2015 年 8 月

摘要

以往「倫敦行動計畫」年度會議討論議題多側重於垃圾郵件及商業簡訊管理、過濾、防護相關法律及技術問題，以及殭屍電腦網路造成的個資隱私洩漏、網路攻擊；在電子郵件仍是網路通訊主流的年代中，垃圾郵件不僅是代表了大量令人困擾的商業廣告郵件，更是網路駭客快速好用的獲利管道，運用社交工程的詐騙郵件尤其是其中重要的工具，透過誘導收信人點擊惡意連結或開啟植入惡意程式之附件，駭客能伺機竊取敏感個資，甚或感染個人電腦成為殭屍電腦，進一步受駭客操縱，進行網路犯罪、網路攻擊之跳板。

本屆「倫敦行動計畫」(LAP；London Action Plan)年度會議於 6 月 8 日至 6 月 12 日在愛爾蘭都伯林市希爾頓 DoubleTree 飯店舉行，為擴充本屆會議議題縱深，會議係由「倫敦行動計畫」、「訊息、惡意軟體、行動通信反濫用工作群組」(M^{3}AAWG；Messaging, Malware and Mobile Anti-Abuse Working Group)兩大組織合併舉辦，使得會議內容涵蓋面由垃圾郵件、商業簡訊濫發、個資隱私安全等層面，討論議題亦跨越至網路安全、資安防護、行動上網等相關議題，在現今行動通信應用快速發展的時代，也更貼近人們的生活討論重心。

而隨著行動通信寬頻技術演進，智慧型手機上網逐漸成為大宗，而配合手機之使用，家用 Wifi 網路資安防護亦逐漸成為重要通訊議題，在家用無線路由器、分享器效能越來越強大及使用情形越來越普遍的情形下，許多網路攻擊事件，事實上與缺乏資安管理的家用 Wifi 脫不了關係。本次會議之議題亦在手機資安、家用網路安全、社交網路部份有所探討。

另一方面，由於 Do Not Call 管理議題在這幾年來，亦為倫敦行動計畫之重要討論議題，故而在會議最後一天，由美國、加拿大、澳大利亞、南韓、印度等國家召開了圓桌會議，共同討論勿來電之管理及防制機制，另外澳大利亞更提出相關國家簽署合作協議之提案。

目錄

壹、前言

儘管我國行政院版「濫發商業電子郵件管理條例草案」仍在立法院中等待審查，國家通訊傳播委員會為配合行政院政策，持續協助推動垃圾郵件防制作為，對外均以積極參與國際反垃圾郵件相關組織活動，尋求擴展國際合作契機方式運作，在國內則持續督促電信事業透過服務契約，提供垃圾郵件技術防制措施，以確保民眾通信權益；進年來，由於垃圾郵件與網路資安議題已密不可分，本會在 104 年度組織改造後，已將防制垃圾郵件工作明確併入電信資安防護工作之一環，除繼續辦理垃圾郵件防制及跨國合作事務，未來將更積極推動電信資安防護事務。本次派員出席倫敦行動計畫，除一方面承續防制垃圾郵件國際合作之交流及擴展任務，促進國際友誼外，另一方面亦藉由參與會議，蒐集、瞭解倫敦行動計畫各會員國對於防制訊息濫用乃至於網路安全防護之未來發展趨勢，以作為本會未來規劃、執行業務之參據。

本次倫敦行動計畫會議，由於係「倫敦行動計畫」、「訊息、惡意軟體、行動通信反濫用工作群組」(M^3AAWG)兩大組織合併舉辦，故而部分議程為同時多軌進行，議題內容包括相關國家垃圾郵件管理、申訴與執法作為、國際組織合作、開發中國家國際合作、對濫發者私權行動、犯罪執法合作、垃圾簡訊、殭屍網路、垃圾郵件與兒少防護、勿來電機制等，議題面向相當廣泛，如能蒐集所有資訊，對於未來各個面向議題之政府政策及管制作為必然有所裨益；然而，囿於公務出國預算限制，本次會議並無法全程出席，且因倫敦行動計畫秘書處將此會議定位於各國政府運作機制之分享，為避免有心人蒐集會議資訊，藉以研析、規避各國政府管理作為，或瞭解法律及執法漏洞而趨避，會議中除宣示不得拍照、錄音、錄影，主辦單位亦不主動索取會議簡報，而係由主講人自願提供方式處理，故而會議資訊蒐集困難。本次報告資料，將針對倫敦行動計畫針對會員公開之會議資料嘗試分析說明，並配合會議要求遮蔽部分資訊，就會議議程、議題內容、檢討心得與建議等項目撰寫，以期提供相關業務之規劃、執行參考資訊。

貳、第十一屆倫敦行動計畫年度會議

一、會議時間、地點及議程

時間：104 年 6 月 8 日～6 月 12 日

地點：愛爾蘭都伯林市希爾頓 DoubleTree 飯店

議程：詳附錄

二、會議議題資料整理

本次會議內容因會議主辦秘書處定義為保密等級，並要求與會者不得拍照、錄音及錄影(限制條款參閱議程)，又會議時間緊湊故而內容單憑記憶可能無法周全，本報告整理之相關資料如欲引用，建議應洽會議主辦秘書處確認為宜。

議題一：跨國執法網絡之整合

與談者：加拿大隱私委員會辦公室代表(OPC；Office of the Privacy Commissioner)，代表 GPEN (Global Privacy Enforcement Network)

美國聯邦貿易委員會代表(FTC；Federal Trade Commission)，代表 ICPEN (International Consumer Protection and Enforcement Network)

英國倫敦國家詐騙情報局代表(National Fraud Intelligence Bureau, City of London Police)，代表 IMMFWG (International Mass Marketing Fraud Working Group)

英國資訊委員辦公室代表(ICO；Information Commissioner’s Office)，代表 LAP

隨著網路消費參與的提升，消費者的網路風險，已由以往的垃圾郵件及殭屍電腦網路，擴大至個資隱私、不實廣告以及行銷詐欺。為了遏阻這些網路犯罪行為，甚或是跨國境網路犯罪，執法行動經常是多個執法機關及目的事業主管機關互相重疊的。

透過本議題邀集 3 大執法網絡代表與談，針對跨執法網絡之協調合作、實務典範、執法工具互享等議題進行探討。

目前各執法網絡均已運作有年，透過執法機關及目的事業主管機關整合為執法網絡之好處包括：可移轉之執法議題倡議、具備較全面性的專業知識、即時與全面性的執法聯繫、易於分享執法工作與實務典範、較有效率之資源取得與運用、較有能力遏阻跨域犯罪行為。而連結多個執法網絡之網路，其主要目標則為透過相關網絡間有效之對話，來提升跨國執法合作。

在此次與談中，分享了 GPEN Network of Networks 計畫，此計畫目的在於透過更有效之對談，促進相關隱私權執法網絡機關間之跨國執法合作，並且建立不同領域間執法機關之聯繫窗口與對談機制，透過此計畫同時提高了 GPEN 成員間取得其他執法網絡之資源及協助。

該計畫藉由一個「聯絡官」的機制，來整合各執法機關間之聯繫，使得相關領域之執法機關與主管機關間有共通之聯繫窗口，來提升各網絡間之互利合作。該計畫規劃將整合 4 個相關網絡，例如：the International Conference、the Berlin Group、歐盟第 29 條資料工作組(WP 29)、倫敦行動計畫等，目前計畫團隊正向倫敦行動計畫、Common Thread Network、Francophone Network、ICPEN 以及 the International Conference 聯繫合作芻議，希望各網絡能同意合作並提供聯絡官名單。本次與談結束，將產生 LAP、GPEN 兩網絡之聯絡官。

議題二：荷蘭網路平臺市場濫用情形

主講者：Delft 科技大學教授

本場次研討會，由主講者提出其針對荷蘭之網路平臺服務業者之資安管理，設計了 1 套基於在有限資源上被濫用資料之安全等級之信用評估計畫，不過該計畫並未考慮平臺業者之大小。

計畫名稱為「Clean NL」，目標為：在網際網路自治系統層級(AS；Autonomous

System)以經驗法則建立「污染地圖」、研究以什麼來區分平臺之好壞、提供典範實務與認知以強化荷蘭平臺市場之自清能力。

計畫之內容由蒐集「StopBadware」、「F.I.R.E」及「PhishTank」等國際反惡意服務相關組織提供之管理不善網際網路自治組織資料進行分析，同時亦比較由 HostExploit.com 取得之資料，而分析後推衍出下表：

頻度	推斷	挑戰
濫用情形發生多頻繁？	示意網路乾淨程度與漏洞多寡	難以再由其他因素來區隔出業者努力程度
濫用情形持續多久？	示意網路處理濫用情形之效率	難以來衡量業者規模

然而要決定濫用情形指標之困難因素如下：

１、如何來測量及統計濫用整治情形：何種濫用情形可被觀察到、整治成效如何界定。

２、與平臺業者之關聯性如何判定：平臺業者之界定範圍、如何標定其規模。

３、如何來控制業者間之歧異：業者大小要如何列入考量、不同之營業模型如何列入考量。

４、如何將不同型態之濫用跡象統計成指標集合。

計畫經討論及分析後，以下列指標來評估荷蘭市場狀態：

１、在不同資料來源上，統計各網際網路自治系統濫用情形發生頻度。

２、以３個方式來正規化自治系統規模。

３、以每個網域名稱或每個ＩＰ位址之濫用次數來對自治系統作成等級。

４、以波達計數法來統計等級分數。

５、以持續高程度濫用之情形來鑑定自治系統。

計畫選取列入分析評估之資料來源包括：

１、濫用情形資料來源：由「StopBadware」、「Shadowserver Compromised Website」、「Shadowserver Sandbox URL」、「Zeustracker C&Cs(Abuse.ch)」、「Mutual Legal

Assistance Treaty(MLAT) requests」、「Dutch Child Pornography Hotline」、「PhishTank」、「Anti-Phishing Working Group」、「Passive Spam Block List(PSBL)」、「Private Spam trap」等組織公布之資料蒐集統計。

2、IP 路由資料：以 Python pysan 程式庫來撰寫 IP 路由分析程式，取出路由資料。

3、被動網域名稱資料(pDNS)：自以下資料中擷取－Farsight Security 提供學界免費研究之 DNSDB、7 億 5 千萬個第 2 階層域名、9 千 3 百萬個 IPv4 網站。

計畫之作業主軸，目前規劃為：

1、結合網路科學研究與執法效益成為反平臺濫用綜效。

2、測量資料來源所觀測網路之污染程度。

3、取得污染程度之低度復原均值。

4、促使更多平臺趨向該均值，強化其自律。

而為了提高指標之正確性，主講者亦針對上述濫用情形指標之困難因素提出協助請求：

1、如何來測量及統計濫用整治情形：希望增加資料來源涵蓋面，加入不同之全球濫用資料源；增加持續時間資料(例如釣魚網站持續運作時間)；研發立論更為堅實之研究方法。

2、與平臺業者之關聯性如何判定：由 WHOIS 層級之 IP 擁有者資料代替本計畫以域名路由層級資料來辨識業者。

3、如何來控制業者間之歧異：由被動域名資料中，擷取業者之剖繪。

4、如何將不同型態之濫用跡象統計成指標集合：對不同統計方法，進行敏感度分析。

議題三：商業騷擾電話－政策比較研究

主講者：Antelope Consulting 代表

本場次研討會，主講者發表其蒐集各國主管機關對於商業騷擾電話之管理政策及相關措施，經比較分析後所見及對相關機關之建議等研究成果，以供與會各國代表參考。

本研究係由 StepChange 債務慈善機構所委託辦理，主講者認為是世界上首見之商業騷擾電話政策研究。研究國家之範圍包括：

1、完整案例研究：澳大利亞、德國、印度、巴基斯坦、英國、美國。

2、較小案例研究：加拿大、荷蘭及挪威。

3、部份資料則蒐集自其他國家。

研究之高層次發現：

1、包括開發中國家，幾乎都有類似且經常發展中之問題(主要為垃圾簡訊)。

2、部份國家比其他國家受害嚴重，然而卻缺乏統計資料(亦無比較性統計)，使得難以與其他國家進行比較。

3、部份擁有很好的實務作為，建議可作更廣泛的推行。

4、國際合作是進步的關鍵。

研究對於目前各國對於商業騷擾電話之管理層次分類如下表：

管制程度	管理機制	國家
低	內部勿來電列表	馬來西亞、烏拉圭、臺灣(僅企業用戶之簡訊)
↓	自主性全國勿來電列表	紐西蘭、瑞士、南非
	義務性全國勿來電列表	英國、荷蘭、愛爾蘭
	義務性全國勿來電列表及註冊機制	澳大利亞、加拿大、美國
高	所有電話行銷均選擇進入	德國、奧地利、以色列

研究亦蒐集各國主管機關之納管情形，並分類如下表：

國家/地區	納管時間	主管機關	主管領域
英國	1999 年	通訊辦公室(Ofcom)，資訊委員辦公室(ICO)	通訊、隱私
美國	2003 年	聯邦貿易委員會(FTC),聯	消費者保護、通訊

		邦通訊委員會(FCC)	
西班牙	2003 年	資料保護辦公室(AEPD)	隱私
德國	2004 年	聯邦網絡管理局(BNetzA)	網路、通訊
愛爾蘭	2005 年	通信監管委員會(Comreg), 資料保護專員辦公室(ODPC)	通訊、隱私
澳大利亞	2006 年	通訊媒體管理局(ACMA)	通訊
印度	2007 年	電信管理局(TRAI)	通訊
加拿大	2008 年	廣播電視與電信委員會(CRTC)	通訊
香港	2009 年	通訊事務管理局(Ofca)	通訊
荷蘭	2009 年	消費者與市場管理局(ACM)	消費者保護
巴勒斯坦	2009 年	電信管理局(PTA)	通訊
義大利	2010 年	MED,資料保護局(GPDP)	通訊、隱私
法國	2011 年	經濟財政產業部(MEF)	消費者保護
比利時	2012 年	SPFE	經濟、糾紛
新加坡	2014 年	個資保護委員會(PDPC)	隱私

另外該研究亦蒐集了各國勿來電登記之情形與申訴之情形，略示如下：

1、登記情形：2014 年美國約 1 萬 8 千戶、荷蘭及澳大利亞約 1 萬 2 千戶、加拿大約 1 萬戶、挪威約 9 千戶、印度及英國約 8 千戶。

2、申訴情形：以每百戶為單位，2014 年美國約 3 件、英國及加拿大約 1 件、其他國家約約 0.2 件。

最後研究結果提出建議如下：

1、對於每個國家：

(1) 對於提升管制作為進行下一步之規劃。

(2) 參考加拿大模式，在充足資源上建立簡單之管制架構。

(3) 參考美國模式，對於違法之嚴重性訂定相對應之罰則，不限於淘汰企業。

(4) 參考荷蘭、挪威模式，嚴格要求電話合約內容之正確性。

(5) 參考印度模式，在勿來電選項方面，促進消費者意識。

(6) 參考法國模式，執行進階低成本網路攔阻措施及簡易申訴。

２、對於所有國家：

(1) 建議分享統計資訊，以便在各國間進行有意義之比較分析。

(2) 參考英國模式，建立垃圾行銷電話與申訴間之比較統計。

(3) 結合執法焦點進行研究，例如「偵查可能性」與「偵查之結果」。

(4) 在呼叫者 ID、跨國調查與執法、誘捕機制方面進行更多合作。

議題四：對於垃圾郵件濫發者之私權行動－增加打擊面

與談人：美國聯邦貿易委員會代表(FTC；Federal Trade Commission)

加拿大工業部代表(IC；Industry Canada)

Nomorobo 組織代表

微軟公司代表

透過私權行動對抗垃圾郵件濫發者是否有效？雖然國際上存在一些打擊垃圾郵件之強力工具，甚或是未被證實有效性之遏阻垃圾郵件軟體；然而仍有反對者認為政府應對垃圾郵件加強執法。本場次座談主要探討，私權行動工具在司法上使用情形並討論其打擊垃圾郵件濫發者之效益。

美國代表在與談中說明美國垃圾郵件管制法(CAN-SPAM Act 2003，Controlling the Assault of Non-Solicited Pornography and Marketing Act)，其立法目的在於管制被濫用之不請自來的商業電子郵件(UCE，unsolicted commercial email)。這些強加在網路存取服務上的垃圾郵件，虛耗了可觀的成本，同時也降低了電

子郵件的可靠性與可用性。而在 CAN-SPAM 法案通過前，由於對於不請自來的成人內容電子郵件沒有要求標示，個人及孩童都可能在非自願情形下打開這些不需要的成人資料。

而哪些行為將構成違反 CAN-SPAM ACT：

１、信首資訊不實或誤導他人。

２、詐欺、騙人的主旨。

３、未依規定標示為廣告郵件。

４、未告知收信人有關發信人之地址。

５、未提供收信人明確方法，對於未來之訊息如何表達拒收。

６、未即時兌現收信人拒收之請求。

７、未監控自已行為寄出之訊息。

８、未對於性內容訊息正確的識別。

可依 CAN-SPAM ACT 提出私權行動之資格：

１、政府機關(如美國聯邦貿易委員會或州總檢察長)。

２、條文 7706(g)之因違法行為受害的網際網路接取服務提供者。

然而依法提出行動，尚需證明受有實際損害，而非僅單純的困擾，或特別是服務提供者在日常服務上微不足道的負擔。

然而該法案認可服務提供者在私權上所謂的損害存在：

１、因增加郵件儲存容量之投注成本。

２、為了處理大量用戶申訴而雇用員工之成本。

３、維持垃圾郵件過濾系統或防制垃圾郵件技術之投入成本。

消費者提出之實際損害，經常與 CAN-SPAM 法案分析無關，主要是因為消費者難以主張其損害，另一方面則是服務提供者提出之主張，在個人資料損失的部份或全部是不正確的。消費者之損害必須打包成在其他方面之花費，例如客戶服務成本等可構成負面影響，以便符合 CAN-SPAM 之法律要件；而對於服務提者，則必須將日常運作費用從實際損害中予以剔除，僅能從因為違法行為

所直接導致必須擴充其儲存容量及系統架構成本方面著手。

由 CAN-SPAM 法案之執行，可以看到，訴訟風險阻止了較小實體之案件提出、消費者損害可能難以量化、法院能夠適應技術的變化(包括社交網路)。

加拿大代表則說明加拿大反垃圾郵件法律(CASL，Canada’s Anti-Spam Legislation)，其監管制度設計包括：新型態違法行為、同意與形式要求、私權請求、行政罰鍰、國際合作、擴充責任，而法案亦包括了全國協調機構、垃圾郵件通報中心之支援機制。

加拿大 CASL 法律規範之新型態違法行為包括：

１、垃圾郵件：不請自來之商業電子郵件。(s.6)

２、駭客行為：未經授權之通訊資料篡改。(s.7)

３、惡意軟體：未經同意安裝電腦程式。(s.8)

４、詐欺：不實或誤導他人表象之網站或網址。(s.75)

５、個資獲取：利用電腦未經同意蒐集電子郵件位址。(s.82(2))

６、隱私侵犯：未經授權存取電腦以在未經同意情形下蒐集個人資料。(s.82(3))

與談者亦談及紐西蘭私權請求(依非應邀電子訊息法案，Unsolicited Electronic Messages Act 2007)：

１、國內執法單位得申請加入行動。

２、法院可對違法行為強加民事處罰並附加賠償(不管是否有損害)。

英國則為依據歐盟隱私和電子通信指令(EC Directive，The Privacy and Electronic Communications Regulations 2003)及資料保護法(Data Protection Act 1998)

議題五：垃圾簡訊之調查－管理機制與案例分析

與談人：紐西蘭電子訊息規管部門資深調查官

藉由本場次研討會來分享紐西蘭垃圾郵件防制機制，包括垃圾簡訊申訴系

統及介紹垃圾簡訊調查實務。

紐西蘭垃圾郵件規管法規為 2007 年立法之非應邀電子訊息法(Unsolicited Electronic Messages ACT 2007)，該法立法目的為－禁止傳送有紐西蘭連結之非應邀商業電子訊息，藉以：

１、提升紐西蘭之資通訊使用環境更為安全及保密；

２、降低紐西蘭商業界及廣大社群近接及有效率使用資通訊之障礙；

３、降低紐西蘭商業界及廣大社群因非應邀電子訊息造成之成本。

該法針對電子郵件、簡訊、即時訊息及傳真，在第 9、10、11、13 及 15 章均有對應之管理規定，主管機關可以對違法者採取下列規管措施：

１、發出書面正式警告。

２、發出民事侵權通知，民事責任事件最高罰款為：對個人 200 紐幣、組織 500 紐幣。

３、接受書面(可執行)承諾。

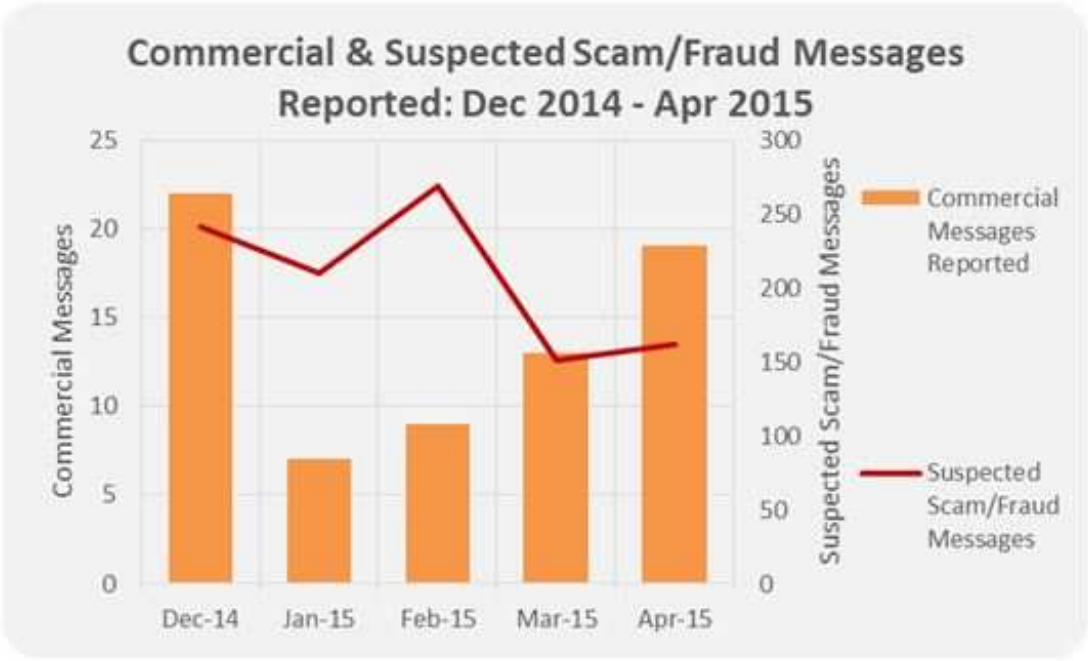
４、透過法院向違法者請求支付罰款：對個人 20 萬紐幣、組織 50 萬紐幣。

５、申請搜查令。

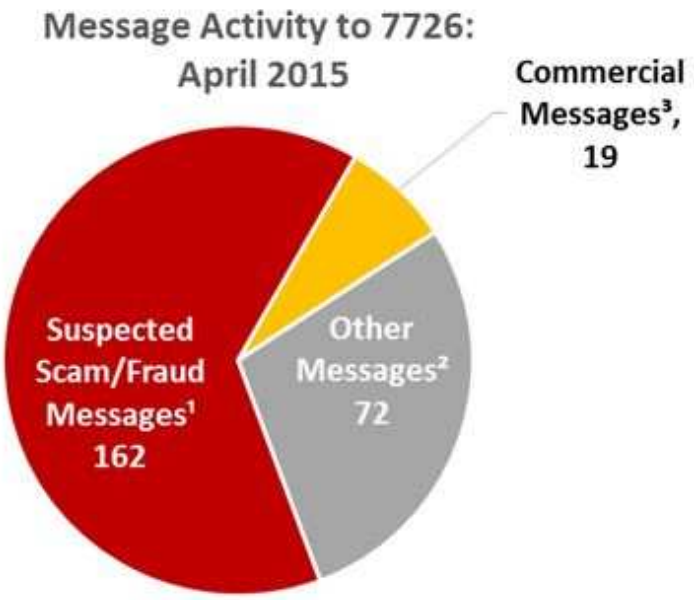
目前該法之民事責任處置情形：發出 449 次書面正式警告、33 次民事侵權通知，接受 2 次可執行承諾，進行 3 次高等法院訴訟、1 次地區法院訴訟，經統計有 11 名累犯。

紐西蘭垃圾簡訊申訴系統，前身為 2007 年之系統，藉由手機及網頁申訴，與主系統目前系統完全不同。2012 年改為網頁申訴方式(7726.govt.nz)，該系統為簡易轉傳並以電子郵件提醒收案。2014 年改為使用 GSMA 及 Cloudmark 合作之垃圾郵件通報服務(SRS，GSMA-Cloudmark Spam Reporting Service)。該系統係由紐西蘭政府與 GSMA、Cloudmark 三方公私合作下催生之系統，具有大量資料聚合、分析能力。

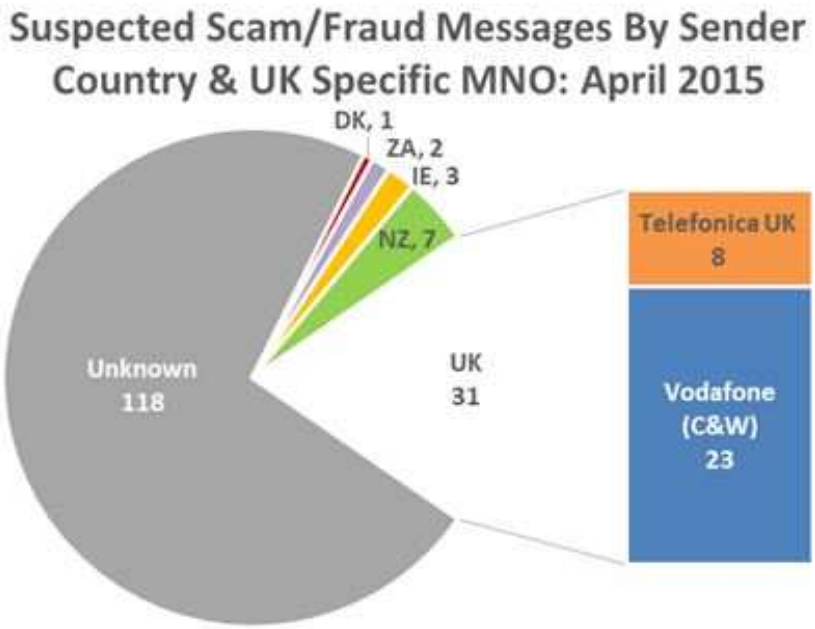
民眾可直接將手機上接收到之垃圾簡訊，以轉發方式，向 7726 舉報，該系統會接收舉報資料，並送至後端之通報服務系統加以分析及處理。而垃圾簡訊可分為騷擾、有害兩種類型，騷擾訊息主要對收訊人造成困擾或不便，有害訊息則可能造成損害(如錢財、精神方面，甚或是對裝置)。7726 收到之申訴案件中，有害訊息每月約在 120 件至 220 件上下，如下圖所示。



以 2015 年 4 月為例，7726 共收到 253 件申訴案件，其中詐欺訊息有 162 件，商業訊息 19 件，其他訊息 72 件，如圖所示。



而這些詐欺訊息中，僅有少數能分辨其來源國家。



因應規管作法：

1、應用各種技術來調查案件，以取得正確資訊；

2、由各個申訴案件中找出變化類型及對應之分析方案；

3、與業界、利益相關者洽商合作；

4、與利益相關者建立雙邊合作關係；

5、以教育方式，向民間及組織提供遵守義務之指引方針；

6、由案件中持續學習及提升調查技術；

7、適當地使用強制措施。

取證注意事項：

1、處理數位證據時依循員警首長協會(ACPO，Association of Chief Police Officers)之指引方針；

2、提升調查用設備之取證能力；

3、致力提升執法人員專業能力。

員警首長協會之數位取證指引方針：

1、執法機關及其人員，不得對於提交法院之資料採取任何行動。

2、如有必要存取原始資料，執行人員必須確認可勝任此事務，且必須能提出證據來解釋採取此行動之關聯及涵義。

3、對於數位證據必須建立並保留稽核資料或所有處理過程紀錄。由獨立第 3 方專業人員必須能檢驗這些程序，且獲得相同結果。

4、負責調查之人員需負全部責任，以確認法律及本指引方針被確實遵守。

對涉案發訊人之詢問(意見陳述)問題：

1、請說明你如何取得發訊資料列表。

2、請舉證說明已取得表列人員同意收訊。

3、特別是+64 開頭號碼，請舉證說明已取得同意收訊。

4、請舉證說明在發出之訊息內有提供有效之解除訂閱功能。

調查實務：

1、透過搜索令在發訊方服務提供者進行搜證，並證實發訊行為，大約 3 個工作天可取得事證。

2、安排涉案發訊人當面意見陳述。

3、對於違法事證，透過法律服務確認違法要件符合。

紐西蘭目前盛行之新型態詐騙簡訊，係以網址結合社交工程方式，誘導收訊人點擊手機上顯示之短網址，發訊者電話號碼則為短碼形式。然而已知部份發訊使用之已發行短碼已經早已過時停用。另外，經查部份網路論壇與垃圾簡訊之廣告軟體有關聯。

為積極管理商業簡訊，紐西蘭政府目前正致力於定時與業者召開會議，討

論簡訊濫用情形之規管工作。

議題六：家用網路之安全問題－個人電腦與手機

主講人：M3AAWG 代表

藉由本場次研討會以淺談方式來分享個人在家用網路中可能遭遇之資安相關議題，嘗試提供自我安全防護相關建議。

安全防護的敵人－複雜度、混亂、驚愕，儲存重要資料之裝置，應有多種安全機制，雖然同時也會造成管理上的痛苦、混亂，但是可避免資料遭竊時之驚愕；而較少的安全機制，雖然對於暫時存放資料較為方便，但是資料遭竊之機率則更高。

密碼－好、壞、醜陋，密碼就像是內衣，不可讓它公開、要定時更換、不要借給陌生人使用，不同用途之密碼，更要避免具有共通性或相似性，以避免因為 1 組密碼的洩露或被破解，導致全面性的損害。

社交、分享與隱私：分享安全－建議關閉網路分享、關閉藍芽探索、關閉自動執行功能,以避免一部份之惡意入侵行為;而社交打卡可能曝露個人地點、生活時序、喜好等隱私，嚴重時亦可能危及人身安全。

中間人攻擊，主要發生在網站瀏覽時之網址重導，有心人可能在網頁中居間竊取資料。

家用網路安全，在使用 Wifi 時 SSID 應考慮安全、唯一性，而開放自動連接將導致安全疑慮；另外，Wifi 控制設定網頁之登入密碼應修改，因為各家廠牌的預設密碼是公開的，駭客可以很輕易的鎖定你所有的通訊，甚或利用你的設備來進行網路攻擊，而你將負擔民事賠償或刑責。

工作時之自攜裝置(BYOD，Bring your own device)、在家中之辦公室裝置－經統計，10%受訪者曾在辦公室違反規定下載，5%受訪者違規存取資安資料，

2/3 受訪者同意他們並不瞭解何謂資安，51%受訪者曾將自己攜帶之設備連接到辦公室電腦，1/5 工作人員讓家人/朋友使用辦公室設備存取網際網路。

議題七：Safety-Net 行動

主講人：防範未經請求商業電子郵件聯盟代表(CAUCE，Coalition Against Unsolicited Commercial Email)

2012 年 6 月 6 日，LAP、M^{3}AAWG 兩大組織會員在德國柏林開會，在同年 10 月，發表了 1 份重要的報告，其中共分為 4 個主要章節，分別有關惡意軟體及殭屍網路、網際網路服務提供者與網址名稱、網路釣魚與社交工程、行動威脅。3 年後，該報告更新為第 2 版，除針對上開 4 個章節內容予以更新，並增加了網路電話及語音電話詐騙、不實來電號碼、主機與雲端服務濫用、網路騷擾等面向之相關內容。

現今網路資訊科技發展迅速，隨著過濾、攔阻技術的進步，網路惡意行為亦逐漸變型，變得更為中性化、更難以分辨，而垃圾郵件已不再是單純的廣告了，更多夾帶惡意資料的情形是常見的。垃圾郵件亦不再是單指電子郵件而已，已隨著科技的進步，擴大至各種型態的新媒體，今日行動簡訊、網路電話之垃圾訊息已是普遍可見，乃至於社交媒體、網誌、網站也被攻占，就連線上搜尋引擎亦充斥垃圾訊息，導致網路搜尋品質的下降。

在網路管理上，其實網域管理機構扮演了極重要的角色，因為垃圾訊息必須存在網路上方能有效提供廣告效果，建議網域管理者應對於網域內之伺服器加強管理，使得網域分類發揮其原本之功能，對於網域濫用的申訴應正視並處理，才能達成把關的管理效果。

惡意軟體在一開始是由電腦技術愛好者所發展的，由挑戰與娛樂的性質，在經濟的促因下，慢慢轉變到犯罪性質，並且開始組織化。惡意軟體偷取個人

或企業資料之方式，大約包括：

１、捕捉按鍵資料。

２、蒐集登入帳號、密碼。

３、拷貝電腦聯絡簿等位址資料。

４、竊取企業、政府、軍事敏感資料、文件。

惡意軟體除了上述偷取資料之活動外，通常亦被用來執行「分散式阻斷服務攻擊」(DDoS)、傳送垃圾郵件、簡訊等。

垃圾郵件是惡意軟體最主要的載體，雖然近年來垃圾郵件即使被引入了新的網路釣魚技術，但是整體來說垃圾郵件之總量已有減少之趨勢，引而代之的是社交媒體上大幅增加了「點擊劫持」、「like 劫持」，當您點擊了網站上的網址時，在幕後可能已被執行了隱藏的惡意程式；知名的網路防毒公司賽門鐵克發現，基於網頁的攻擊事件，2013 年比 2012 年上升了 23%，網路上約 1/8 的網站具有弱點，使得透過網站來傳遞惡意軟體已經比透過郵件更加具有資安威脅。2015 年，惡意軟體更發展至「勒索」威脅。

對抗惡意軟體，個人應該：

１、選擇使用安全、新的作業系統。

２、經常性執行系統、軟體更新，減少已知漏洞存在的可能性。

３、刪除不用的軟體，避免下載、安裝不必要的軟體，以減少外來風險。

４、尋求專家協助。

５、使用有效的防毒軟體，並定期掃毒。

６、使用防火牆，提高防護能力。

７、使用較安全密碼，避免易於被他人猜中。

８、經常備份資料，降低資料損毀時之困擾。

９、刪除不用之暫存檔案，提升系統防毒、備份效率。

１０、 經常性工作避免總是使用最高權限帳戶。

１１、 瀏覽網頁時，儘量關閉 JavaScript 功能，減少惡意網頁幕後執行之機會。

１２、 阻擋並避免瀏覽已知之惡意網站或網域。

１３、 濾除可能有害之電子郵件。

１４、 儘量減少下載 P2P 檔案。

１５、 使用 USB 要加強注意可能已被感染惡意軟體之風險。

１６、 避免使用陌生的 Wifi 熱點，因為通訊可能被監聽。

而有些跡象應該要特別小心：

１、防毒軟體之病毒偵測提醒，可能是外來入侵已進入的警告。

２、如系統反應開始怪異，小心系統可能已被入侵者操控。

３、如果你的網路服務提者通知你，你的系統已被檢舉從事不當網路行為，應該要立即配合採取挽救行動了。

損害控制：

１、開始清理系統，掃毒、刪除不必要的軟體

２、回復上次正常的系統備份。

３、乾脆重新安裝系統，並立即更新系統。

網路釣魚常見於電子郵件、簡訊，甚或是帶有網路鏈結之任何電子訊息，主要為重導收訊者到偽造的網頁，而表徵則為要求輸入或更改帳號、密碼，或要求信用卡資訊等個人敏感資料。在美國，2015 年第 1 季就發生了約 1 億 2 千萬筆病患個人紀錄被竊事件。

以下為 4 種常見的網路釣魚型態：

１、 電子訊息中包含有重導位址鏈結，出現之網頁多為偽造之金融、商務、電郵網頁，並要求您登入。

２、 含有網頁型態附件之電子郵件，其呈現方式為表單，並需要您輸入相關個人資料。

３、 提供電話號碼列表或鏈結，並要求您點擊或呼叫。

４、 簡單的回應訊息，並要求驗證您的身分或回應此訊息。

行動裝置惡意軟體，目前以 Android 系統為主要對象，通常由網站或非正

式 APP 商店散佈，而通常，惡意軟體散播者係以破解合法 APP，並置入惡意程式碼方式進行，透過破解免費或提升功能方式吸引受害者下載安裝。

2014 年發生了「SMS Worm」惡意軟體，透過簡訊散播，主要為感染手機通訊錄，並向聯絡人發送惡意簡訊以加速散佈。

行動惡意軟體常見的活動包括：

1、 向聯絡人發送短網址簡訊。

2、 下載付費內容、點擊付費鏈結。

3、 盜撥高額付費電話。

4、 攔截網路銀行認證資料。

5、 鎖定行動裝置並勒索解鎖費用。

6、 蒐集聯絡人資料，發送垃圾簡訊，蒐集個人資料、監視個人喜好作為行銷用途。

7、 強迫顯示廣告資訊。

8、 盜用裝置運算能量。

對抗行動惡意軟體，建議作法如下：

1、 教育消費者，不使用來源不明、信用評等有問題之 APP。

2、 提醒消費者，安裝 APP 時應詳細檢視並瞭解 APP 要求之權限是否合理。

3、 教育消費者，維持裝置預設之安全限制，不可破解安全限制。

4、 安裝由遠端可定位及上鎖之防護軟體，以便在裝置遺失時保護資料。

5、 安裝及執行安全防護軟體。

6、 鼓勵消費者舉報可疑軟體。

7、 對於行動裝置資料建立備份。

網路不當內容造成之網路騷擾，一向是重要課題，由於網路具有一定匿名性，導致網路上常出現社會脫序行為，其形式包括：

1、 交友詐欺－以假個資在交友網站及社交媒體活動，詐欺他人錢財。

2、 分類詐欺－以假廣告刊登尋求訊息，詐欺取得他人之電話號碼或電郵位

址。

3、 網路霸凌－在網路上透過網站、社交媒體、留言板、電子郵件等相關媒體，對他人進行文字或言論攻擊或排擠。

4、 網路干擾－透過網路通訊方式不斷騷擾他人。

5、 網路曝光－將他人可供辨識之隱私資料，於網路公開。

6、 假扮他人詐欺－利用他人資料於網路假扮他人，發布訊息以侵害該人信用或詐騙錢財。

7、 網路排擠－利用網路群體力量干擾受害人，期使其從網路驅離或遭退學或失去工作。

8、 隱私洩露－未經許可，在網路上揭露他人隱私資料，例如病史、性愛好等。

9、 線上認證竊取－竊取他人認證資料，以代他人進行金融貸款或融資，使他人蒙受損失。

10、 復仇批判－在網路發布對他人不利之假訊息，並以嚴厲方式批判他人。

11、 復仇式公開不雅照－未經他人允許,在網路發布他人不雅照片、影片，以損害他人名譽。

12、 自拍不雅照－在網路發布自拍不雅照片、影片，主要為對不願接收者造成侵擾。

13、 假報案－捏造假犯罪情形，向警方舉報他人涉及犯罪，以透過警方調查行動干擾受害人。

14、 網路小白－在網路發布針對性論點或訊息，引發他人不滿或爭論。

對於網路騷擾行為，建議個人於上網時應儘量：

1、 限制個人資料之公開－避免於網路公開過多可辨識個人之資料，多少可以減少不必要紛爭在個人身上發生，避免有心人不當利用。

2、 避免情勢不斷升高－當遭受網路霸凌時，避免隨之起舞，依事態考慮忽

視之。

3、 紀錄霸凌行為－對於網路霸凌行為，保留過程事證，包括電子及紙本形式，以便可行時訴諸法律。

4、 向主管機關舉報網路霸凌－網路雖有一定匿名性,但仍有通信紀錄可稽，網路不當言論或行為仍受法律規範，向警方報案是解決問題的良好起點。

5、 管理上網狀態－上網時應保留一定程度隱私，例如在社交媒體，應限制所有網路 po 文僅能被朋友看見，而不是全部公開。

6、 加強密碼強度－避免在各網站間使用相同密碼，以避免網路身分遭他人盜用。

7、 保持良好上網行為習慣－網路行為有一定程度會影響他人，在上網時儘量維持良好行為，可避免致生不必要糾紛。

議題八：南韓手機垃圾郵件誘捕系統

主講人：南韓資訊安全局代表

為了對抗南韓手機垃圾郵件濫發行為，資訊安全局開發了一套誘捕系統，使用全新的行動電話號碼來蒐集、分析並且立即阻擋傳入之垃圾語音/簡訊訊息，而蒐集到之訊息則用來處罰濫發者。

雖然南韓已立法規範濫發行為，然而事實上很難去釐清收訊者是否有同意發訊者願意接收訊息。此系統之所以使用全新的號碼，用意即在發訊者絕不可能取得同意收訊，因該號碼係資訊安全局所擁有，任何傳入之垃圾語音/簡訊訊息必然違法。

此系統記錄垃圾語音訊息之格式如下：

日期	來電號碼	收訊號碼	型態(語音/自動系統)	來電秒數	紀錄檔名

系統記錄垃圾簡訊訊息之格式如下：

日期	來電號碼	回應號碼	收訊號碼	訊息內文

行動電話業者配合在垃圾簡訊傳入時，協助：

1、 在接收垃圾簡訊時，行動電話業者將簡訊內容以電子郵件寄給資訊安全局。

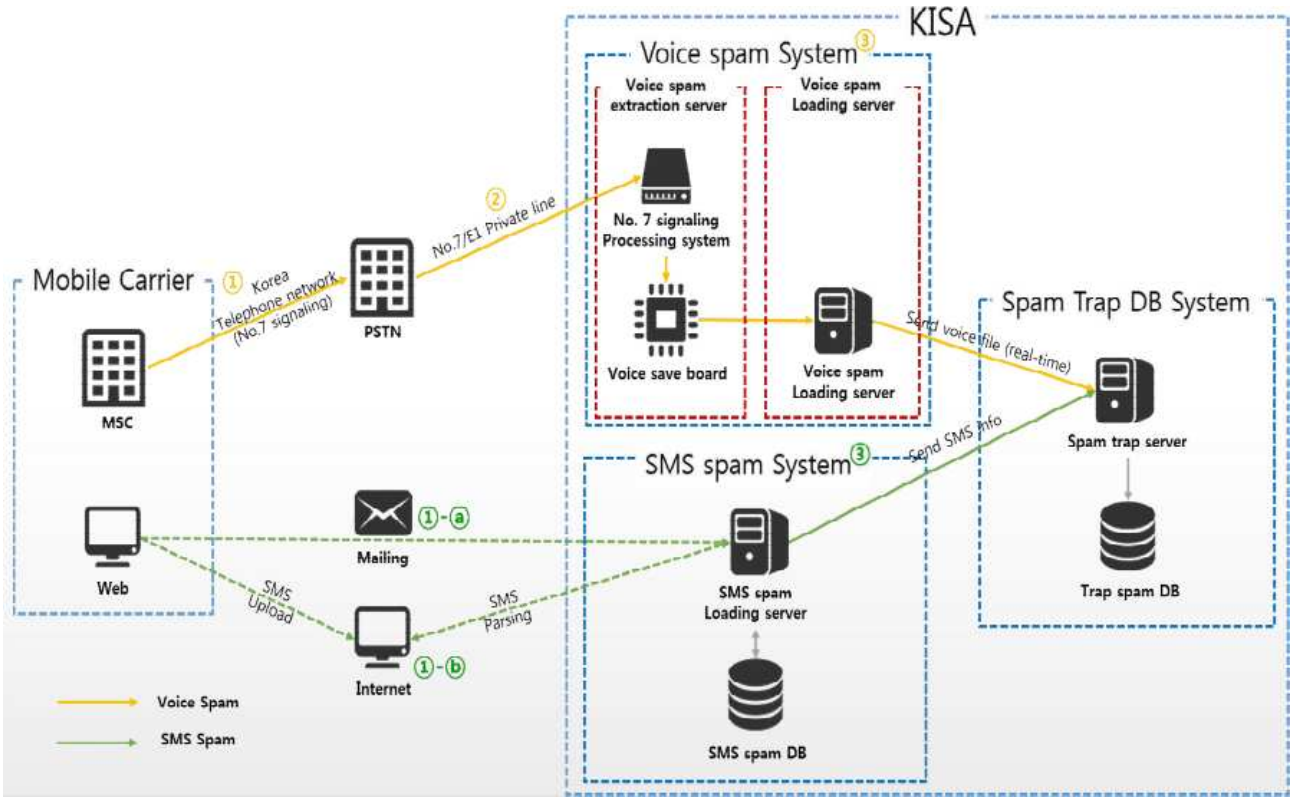
2、 垃圾簡訊首先存在行動電話業者之資料庫中，當資訊安全局透過網頁存取後，存至資訊安全局之資料庫中。

目前系統遭遇之問題：

1、 如果發訊者使用造假的行動電話號碼，則難以找到發訊者。

2、 系統對垃圾簡訊之阻擋非常有效，但是垃圾語音訊息則很難，因為系統對於內容之判斷無法如同人一般精準。

以下為系統方塊圖：



議題九：南韓垃圾郵件立法及目前規管情形

主講人：南韓資訊安全局代表

南韓垃圾郵件法律規管重點包括：對電子媒體(包含語音、傳真、電子郵件等)傳輸以擴充式選擇進入機制管理、要求遵守標示義務(訊息開頭標示 ADV，並提供發訊者姓名及連絡資訊)、賦予資通訊服務提供者拒絕提供垃圾郵件傳輸服務之權利。

法律要求資通訊服務提供者必須在網路層次採取阻攔垃圾郵件行動，否則服務提供者即為違法。

南韓手機上之垃圾郵件，在 2010 年達到高峰，約有 7 千萬封，之後每年逐漸下降，2014 年大約有 1 千 5 百萬封；不過惡意垃圾郵件並未明顯減少，主要是因傳送路徑多樣化而且多為智慧型傳送。

目前手機垃圾郵件傳輸技術有大幅提升情形：

1、 透過傳送影像垃圾郵件、語音垃圾郵件以規避服務提供者之阻攔。

2、 由於收訊者除了數據使用費外，接收一般簡訊/多媒體簡訊無需費用，所以濫發者發送大量之一般簡訊/多媒體簡訊，以提高投資報酬。

目前南韓之語音垃圾郵件增長快速，2014 年第 1 季僅 21 萬封，2015 年第 1 季已增加到 151 萬封。

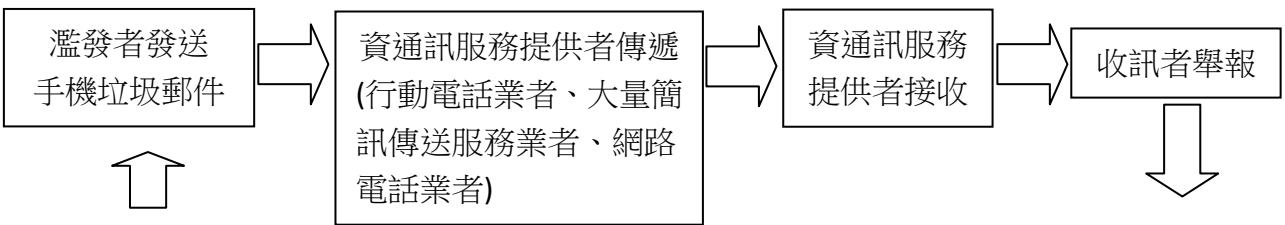
目前進階之手機垃圾郵件傳輸技術流程：

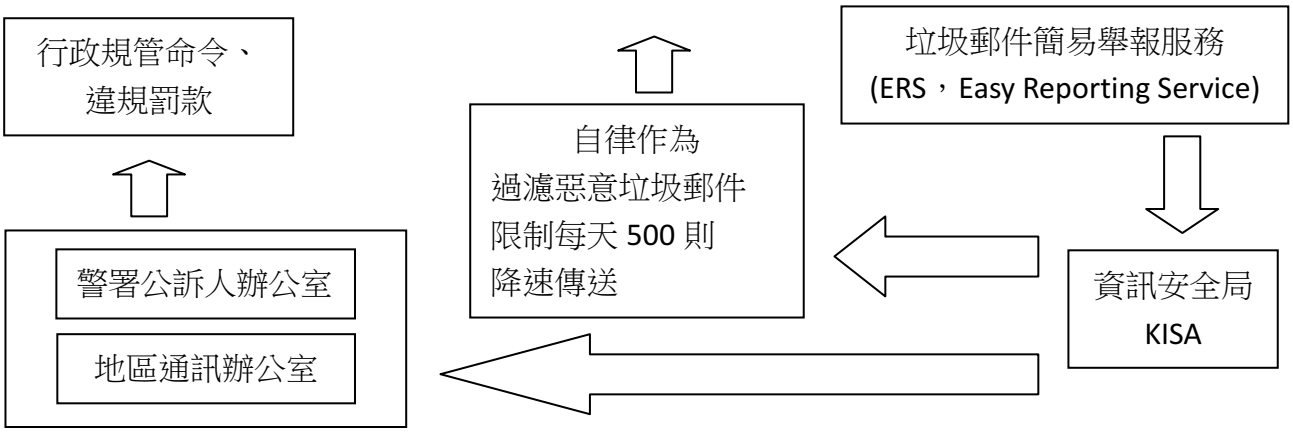
1、 大量購入二手行動電話，安裝發送一般簡訊/多媒體簡訊之 APP。

2、 使用電腦來發動 APP。

3、 透過 Wifi 熱點傳送。

南韓之手機垃圾郵件規管簡化流程如下：





為促使業者加強防制垃圾郵件，南韓自 2012 年起並分析、公告主要資遢訊服務提供者之垃圾郵件散播量，包括：接收垃圾郵件量、傳遞垃圾郵件量、行動通信業者簡訊接收量/垃圾郵件實際攔阻量。

為服務民眾，南韓在手機上開發 APP(ERS，Easy Reporting Service)，供民眾舉報手機垃圾郵件，當民眾收到手機垃圾郵件，可透過該 APP 立即向行動通信業者舉報，業者確認通訊紀錄後，即將相關資料一併傳送至資訊安全局之蒐集系統，由該系統進行下一步處理。

為強化垃圾郵件防制作為，南韓於 2013 年再度開發了一套全面性的監測及分析系統，將資訊安全局接收之手機垃圾郵件報告及行動通信業者之垃圾郵件黑名單整合，進行即時分析並提供行動通信業者加強管理。資訊安全局並於整合後，即時提供各家行動通信業者更新黑名單，使之成為即時黑名單機制。

另外南韓資訊安全局亦建置了手機垃圾郵件誘捕系統，由各家行動通信業者提供未曾配發使用之行動電話號碼給資訊安全局，當濫發者發送語音/簡訊垃圾郵件至該門號時，即被系統捕捉並進入分析、處罰之機制。

為防遏影像垃圾郵件，南韓亦建構了影像垃圾郵件防堵系統，透過智慧型分析及整合資料庫，同時與行動通信業者合作防堵，目前已可作到 7.2 秒攔阻之效率。

有關語音垃圾郵件部份，經由民眾舉報後，進入資訊安全局系統加以分析並建立即時黑名單，再傳送至行動通信業者，由業者負責即時攔阻。

參、心得與建議

歷年來，倫敦行動計畫之年度會議如在歐洲舉辦，通常均會與「訊息、惡意軟體、行動通信反濫用工作群組」(M[3]AAWG)組織合併舉辦，議程內容及面向將會配合擴大至網路、通訊資安等相關層面，議題亦較為多元，可能及於兒少、網路內容防護；如僅為倫敦行動計畫獨立舉辦，則議程多侷限於垃圾郵件、垃圾簡訊、網路詐欺，面向似有偏向消費者保護之情形，而且多以邀請各國座談方式辦理，究其原因，應係多數倫敦行動計畫會員為消費者保護主管機關之故。然而不管以何種形式舉辦，對於打擊垃圾郵件、遏阻訊息濫用來說，都是一個非常重要的交流平臺。本次出席之會議即為兩大組織合辦之形式，議程天數長達 5 天，討論議題相當豐富，對於從事相關業務來說，可以藉由相關議題分享，參考他國業務處理經驗及提升自身技術能力；另一方面，透過與各國執事人員交流，除分享知識與經驗外，亦可建立國際聯繫能量，有助於未來擴展國際合作。

雖然防制垃圾郵件議題，對於資訊科技發達的已開發國家來說，已不是最重要的政策方向，然而對於部分新參與倫敦行動計畫的國家，仍抱持積極態度參與，與會官員之層級亦相對較高，例如本次會議，各國多為事務官員參與，最高為處長層級，而南非則由其消費者委員會(NCC, National Consumer Commission)副主任委員出席會議並參與座談，突顯該國在消費者權益保護方面對於濫發訊息相關議題關心程度。

就我國而言，其實政府開始關心垃圾郵件問題之時機並不算太晚，因為加拿大之垃圾郵件管理法也遲至 103 年 7 月才生效，然而在我國長久的推動立法過程中，卻因多方考量因素及產業界反對立場，導致法案規劃之管理範圍並未因時俱進，配合通訊科技之發展而有所修改，致使其他國家已可針對廣泛的商業電子訊息濫用行為施以管制時，我國仍僅能針對垃圾郵件考慮加以管理，亦導致專家學者多有認為此為落伍之立法政策，以技術層面管理即可處理此議題。然而就撰文者看來，因為沒有法律明確規範，致使在政府推動防制作為時，無法可依為行政，推動實務上經常會遇到困難，所謂的技術防制，透過行政指導仍必須視業者在考量成本、效益及用戶反應之後的綜

合態度而定，故而目前業者採用的多是過濾率約 85%上下之垃圾郵件過濾系統，並以業者基於成本考量認為適當的人力配置來執行，而在服務契約方面，亦未必配合防制需要增列管理濫發行為之授權條款；另一方面，業者為避免糾紛，在執行上除非有明確事證且由相關機關正式通知，否則不會立即對濫發行為停權處置，導致規範機制效率不高；甚或有因未提供電子郵件服務，故而無法配合推動技術防制垃圾郵件作為。其實不只是垃圾郵件，目前在用戶資安防護方面亦遇到相似之問題，建議能儘速訂定資安法規以利遵循，俾利在資安事件發生時能更有效對於違法行為加以規範。

近來本會配合通訊傳播匯流趨勢，正在研議修訂匯流相關法規，審酌行政院版「濫發商業電子郵件管理條例」草案即將因立法委員任期屆滿而屆期不連續，在即將面臨重新研議規劃之際，建議能有明確政策方向，思考順應世界各國規管趨勢來訂定新規範，例如即以商業電子訊息濫發行為為規管對象，授權主管機關因應科技發展，指定其規管範圍，回歸民法侵權機制，主管機關則針對重大違法行為或常業犯加以行政管理，並致力國際合作，以有效運用有限行政能量，維護民眾通訊權益。

如未來能順利通過立法管理濫發商業電子訊息行為，在手機垃圾郵件方面建議可參研南韓之即時防制相關機制，其面向已相當完整且與業界之自律作為相互扣連，在防制實務上已達到即時反應處理之程度，實屬值得詳細研究學習，相關作為如獲採行，當可有效防遏濫發行為，維護通訊環境之暢通與秩序。

肆、附錄

一、議程

LAP Dublin: Progress through Partnerships

All Sessions Will be in Meeting Rooms 1 & 2 Unless Otherwise Noted

Monday 08 June 2015 - Registration with LAP/MAAWG

2:30 – 6:00 **Investigating Spam cases: LAP Training (Toni Demetriou to organize with University College Dublin)**

Tuesday 09 June 2015

LAP Sessions

7 – 8:30 **Breakfast**

8:30 – 8:45 – **Introduction: LAP Secretariat**
Steve Eckersley ICO (UK) Betsy Broder FTC (US)

8:45 – 9:15 – Keynote Address
Manon Bombardier, Chief Compliance and Enforcement Officer, CRTC (CA)

9:15 – 10:30 **UK and Irish Approaches to Managing Spam**
The Office of the Data Protection Commissioner will outline the Irish approach to processing complaints regarding unsolicited marketing telephone calls and text messages, the Commissioner's legal powers, its prosecution strategy, case studies in relation to prosecutions and its media strategy. The UK Information Commissioner's Office will address their approach to taking enforcement action in this area, including details of recent warrants exercised and other action taken.
Discussants: Steve Eckersley, Information Commissioner's Office (UK)
Tony Delaney, Assistant Commissioner, Data Protection Authority (Ireland)

10:30 – 11:00 Break

11 – 12 **Chairman Opening and JD Falk Award (With MAAWG)**

12 – 1 **LUNCH**

1 – 2 **Networking the Networks: Making Sense of Alphabet Soup**

Online risks to consumers range from spam and botnets, to privacy, misleading advertising and mass-marketing fraud. Many of these threats involve significant overlap among enforcement and regulatory authorities and their respective multi-national networks. This session will consider how to leverage the best practices, tools and approaches of networks such as LAP, GPEN and the IMMFWG, through the encouragement of a global, inter-network, dialogue.

Discussants: **Adam Stevens (UK ICO) *LAP***
Brent Homan OPC (Canada) *GPEN*
Jonathan Frost National Fraud Intelligence Bureau, City of London Police, *IMMFWG*
Betsy Broder, FTC, *ICPEN*

2-3 **Building Bridges with Developing Economies**

The Internet has linked the world in ways thought unimaginable 25 years ago. Progress is not even, though, and many economies remain burdened by spam, botnets, inadequate bandwidth and other impediments to a resilient Internet. This panel will explore the challenges faced in different economies, searching for practical solutions to deliver on the promise of a connected and robust global network.

Moderator: **Andre Leduc, Industry Canada**
Panelists: **Monika Josi, SAFIS (Switzerland)**
Thezi Mabuza, National Consumer Commission, South Africa
Robert Ravi, TRAI (India)
Jerry Upton, MAAWG Foundation

3 – 3:30 **Break**

3:30 – 4:30 **Private Rights of Action Against Spammers: Adding cops to the beat**

Are private rights of action against spammers effective? Although some strongly support such measures as part of a broader set of tools to fight spam, others are indifferent, citing the unproven effectiveness in deterring spam, while still others oppose them on the grounds that government is better placed to enforce laws against spam. This panel will explore the private right of action tool as defined and/or used in their jurisdiction and discuss its benefits in the fight against spammers.

Moderator: **Betsy Broder, FTC**
Discussants: **Andre Leduc, Industry Canada**
Aaron Foss, Nomorobo
John McHugh, Senior Manager EMEA Investigations, Digital Crimes Unit, Microsoft

4:30 – 5:30 **2020: Welcome to a Spam-Free World! How did we get here?**
What we know: M³AAWG and LAP played a key role in this amazing achievement. Something else happened, something which had never been thought of, tried or done before 2015. Come and share your most game-changing and audacious ideas to tackle the spam problem!
Moderator: Jean-Christophe Le Toquin, Socogi (FR)
Discussants: Pepijn Vissers, Authority for Consumers and Markets (NL)
Betsy Broder, FTC

Wednesday 10 June 2015
LAP Sessions

7 – 8:30 **Breakfast**

8:30 – 9:30 **Coordinating with Criminal Enforcement Authorities**
When regulatory and civil enforcement actions are not enough to stop spammers, it may be time to call in the criminal enforcement authorities. Hear from regulatory authorities and industry on when and how to call in the "big guns."
Moderator: Betsy Broder
Panelists: Jonathan Frost, City of London Police
John McHugh, Microsoft
Inspector Michael Gubbins, Computer Crimes Investigation Unit, An Garda Siochana

9:30 – 10:30 **Affiliate Marketing: SMS Spam**
In affiliate marketing, suppliers establish a relationship with another business to promote their marketing activities. Although this can be done properly, in the SMS space, the messages often fall on the wrong side of the law. This panel will consider the problem by looking for synergies across jurisdictions with a view to reducing consumer harm.
Moderator: Julia Cornwell-McKean, ACMA,
Discussants: Toni Demetriou, Department of Interior, New Zealand,
Adam Stevens, ICO
PPP (by teleconference, if possible)

10:30 – 11 **Break**

11 – 12 ***MAAWG KEY NOTE***

12 – 1 **Lunch**

Programming with MAAWG

1 - 2 **Economics of Botnets**
Michel Van Eeten, Delft University (With MAAWG)

2 – 3 **Spam and Child Abuse Material: The connection**
The antispam community can play a vital role in stopping the distribution of Child Abuse Material (CAM). This workshop will give the knowledge to deal with a CAM incident on your network, and will help you understand the impact of your actions, when dealing with an incident, on the child, law enforcement, your fellow professionals and your organisation.
Discussants: Jean Christophe LeToquin,
Mick Moran, Assistant Director Human Trafficking and Child Exploitation, Interpol
Paul Vixie, CEO, Farsight Security

3 – 3:30 **Break**

4:30 – 6 **OPERATION SAFETY-NET: BEST PRACTICES TO ADDRESS ONLINE, MOBILE, AND TELEPHONY**
In October 2012, LAP and M³AAWG prepared and submitted to the OECD Consumer Protection Committee a plain language report entitled "Best Practices to Address Online and Mobile Threats." Often referred to as the *OECD Best Practices Report*, it was one of the first, and best, global efforts to encourage the adoption of best practices to address a variety of online and mobile challenges.

Much has changed in the three intervening years. With the input from more than 100 industry and public sector leaders, the collaborative has produced a revised version, which includes updates to the four original sections, and added discussions of VoIP fraud, Caller ID Spoofing, abuse issues at Hosting and Cloud Services Providers, and a side-bar focused on online harassment. Among the current problems we are addressing are DDoS attacks and data breaches.
Discussants: Neil Schwartzman (CAUCE), Andre Leduc (Industry Canada)

MAAWG Night Out - Bus loading at 6:30

Thursday Morning – LAP Business Meeting

8:30 – 9:30 **Committee reports**

9:30 - 10:30 **Planning Session**

!0:30 – 11- **Break**

11 – 12 – **LAP Wrap up and Planning for LAP 2016**

Do Not Call Enforcement Network
Thursday afternoon

1 – 4 LAP and VTA SIG -- Joint Do Not Call Roundtable
Alex Bobotek AT&T
Manon Bombardier – CRTC
David Gibson – CRTC (Via telecon if poss)
Patty Hsue FTC

Friday Morning – Do Not Call

8:30 - Introduction – Julia Cornwell-McKean and Tom Lowry

8:45 – 9:30 Honey Pots – a tool for law enforcement
Patty Hsue - FTC (US)
Max Choo, Spam Response Team, Manager KISA (Korea)
Insu Jo, Spam Response Team, Deputy General Researcher, KISA (Korea)
Kelly-Anne CRTC (Canada)

9:30 – 10:15 Enforcement update and Robocall sweep
William Maxson, FTC
Steven Eckersley, ICO
Tom Lowry CRTC
Robert Ravi, TRAI (India)

10:15 – 11 - DNC MOU
Julia Cornwell-McKean – ACMA

11 –12 Committee Reports

1 Concluding Remarks

本次會議內容因會議主辦秘書處定義為保密等級，並要求與會者不得拍照、錄音及錄影(限制條款參閱議程)，本報告整理之相關資料如欲引用，建議應洽會議主辦秘書處確認為宜。

Reminders for Our Worldwide Friends

All meeting content is confidential: No photos, no video, no recording.
See staff with questions.

L'ensemble du contenu de la réunion est confidentiel: les photos, vidéos et enregistrements **sont** interdits. Pour toute question, demandez conseil au personnel.

Todo el contenido de la reunión es confidencial: No está permitido sacar fotografías ni grabar vídeo o audio. Consulte con el personal si tiene alguna pregunta.

Der gesamte Inhalt des Meetings ist vertraulich: Keine Fotos, kein Video, keine Tonaufzeichnung. Bei Fragen wenden Sie sich an die Mitarbeiter.

会議の内容はすべて機密扱いです。写真やビデオの撮影、録音は禁止されています。質問がある方は、スタッフまでご連絡ください。

所有会议内容均为保密信息：禁止拍照、录像、录音。如有疑问，请咨询职员。

회의에서 다루는 모든 내용은 기밀입니다. 사진 및 동영상 촬영과 녹음은 금지됩니다.
질문이 있으시면 직원에게 문의해 주십시오.

Attendees Reminder:

What occurs in a M³AAWG meeting cannot be shared outside the membership

- Blogging, tweeting, posting is NOT allowed EXCEPT for referencing or citing the specific content on official M³AAWG public sites, which can be reposted or used in articles. The official sites are: www.m3aawg.org/DM3Z, www.Twitter.com/maawg, www.Facebook.com/maawg, https://www.facebook.com/groups/maawg/
- Respect M³AAWG anonymity: No publishing people or company names, except as cited on the official M³AAWG channels listed above
- No use of Wireshark or similar products on the M³AAWG network
- No photography - No video - No audio recording
- Any exception requires written permission from the Executive Director and may require permission from the session members
- All meeting attendees must wear and have their M³AAWG badge visible at all times during the meeting
- Please silence all electronic devices; be courteous to those listening to the presentations
- DO NOT LEAVE YOUR BELONGINGS UNATTENDED. Be aware and cautious at all times.

Treat all attendees respectfully in and out of sessions. No less will be tolerated.
Please review our meeting Conduct Policy at http://www.m3aawg.org/page/m3aawg-conduct-policy

For questions, please contact Jerry Upton at: jerry.upton@m3aawg.org