

國立交通大學

管理學院

碩士在職專班科技法律組

碩士論文

論文題目: **The Study on the Trend and Enforceability
of Regulations Governing Unsolicited Commercial
Emails**

(中譯: 未經邀約的電子郵件規範趨勢及可行性之
探討)

研究生: 楊敏玲

指導教授: 王敏銓 教授

中華民國九十六年十二月

The Study on the Trend and Enforceability of Regulations

Governing Unsolicited Commercial Emails

中譯：未經邀約的電子郵件規範趨勢及可行性之探討

研究生：楊敏玲 Student: Min-ling Yang

指導教授：王敏銓 教授 Advisor: Min-Chuan Wang

國立交通大學

管理學院碩士在職專班科技法律組



**Submitted to Institute of Technology Law
College of Management
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master
In
Technology Law**

December 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年十二月

**The Study on the Trend and Enforceability of Regulations Governing
Unsolicited Commercial Emails**

Student: Min-Ling Yang

Advisor: Dr. Min-Chuan Wang

**Institute of Technology Law
National Chiao Tung University**

ABSTRACT

This Article is divided into three parts. Part one is an introduction of spam, explaining the problems caused by spam, who profits from spam, and how spammers collect email addresses. Moreover, it contains some cases to analyze the conflicts between freedom of speech and privacy. Part two quickly sketches the three-part responses to spam by Internet Service Providers (“ISPs”) and businesses: self-regulation, technological innovation, and legislation. Additionally, developments in recent litigations will also be included. Part three will introduce EU’s attitude towards spam and its opt-in rule. Furthermore, I will address the consequences of the Organization for Economic Cooperation and Development (“OECD”) on spam. Part three will discuss and analyze whether it is necessary to enact an exclusive law on spam in Taiwan.

未經邀約的電子郵件規範趨勢及可行性之探討(中譯)

學生: 楊敏玲

指導教授: 王敏銓教授

國立交通大學管理學院碩士在職專班科技法律組

摘要

本文主要分為三部份，第一部分為簡介何謂未經邀約的電子郵件(SPAM)及其可能造成問題，並說明在寄送 SPAM 中，獲利者為誰及這些人如何收集個人資料來寄送 SPAM。此外，此部分將會藉由分析案例來說明言論自由及隱私權的衝突。第二部份將會說明 ISP 業者及其他業者如何對抗三種方式: 自我管理、科技發明及立法，並簡介近代對 SPAM 的立法過程。第三部份將會簡介歐盟對抗 SPAM 的態度與其採用 opt-in 方式，並說明 OECD 對於 SPAM 所採取方法，最後，本人將提出及分析我國是否有必要制定對抗 SPAM 專法。



誌 謝

當碩士論文口試結束一剎那，內心是百感交集，高興的是終於結束了一邊辛苦唸書及工作的日子，感傷的是同學見面的機會漸漸變少。交通大學管理學院在職專班科技法律組這四年來日子，一幕幕浮現在我的眼前，感謝劉尚志所長像大家長般地，關心所上每一位學生，為大家爭取各項資源及福利，感謝王敏銓老師在我們快要放棄寫論文時，固定安排討論時間，督促我們完成，感謝我的好友陳冠宇在交大上課這段時間，每週六載著夜歸的疲累的同學們回家，感謝各位同學與我在交大共渡每一個日子，讓我留下人生美好回憶，感謝我的雙親默默地在我背後給予力量與勇氣，感謝我的先生張志銓默默地陪伴我完成許多報告及作業，最後，感謝一路上許多相助貴人，讓我人生因為你們而更豐富。

The Study on the Trend and Enforceability of Regulations Governing Unsolicited
Commercial Emails

(中譯：未經邀約的電子郵件規範趨勢及可行性之探討)

Min-ling Yang

English Abstract.....	ii
Chinese Abstract.....	iii
Appreciation.....	iv
Content	
Preface.....	1
Chapter 1. The Problem of Unsolicited Commercial Emails.....	1
1.1 The Problem of Unsolicited Commercial Emails.....	1
1.2 What is Spam?.....	1
1.3 A fast, Convenient and Effective Marketing Tool.....	2
1.4 How Can Spammers Acquire Your Email Accounts and Private Information?.....	3
Chapter 2 The Conflict with Freedom of Speech.....	4
2.1 Freedom of Speech.....	4
2.2 Pornographic/Obscene Speech.....	6
Chapter 3 The Three-step Responses to Spam.....	7
3.1 Self-regulation.....	7
3.2 Technology Innovation.....	8
3.3 Legislation.....	9
Chapter 4 The CAN-SPAM Act.....	11
4.1 History.....	11
4.2 The Definition of Commercial Electronic Mail Messages.....	12
4.3 Relevant Regulations.....	12
4.4 Law Suit and Damage.....	14
4.5 Mobile Spam.....	14
4.6 Relevant Cases.....	15
4.7 The Enforceability of National Do Not Email Registry.....	16
4.8 Do Not Email Registry Report.....	18
4.9 Conclusion.....	19
Chapter 5 The Spam Solution of the EU.....	20
5.1 The Attitude of the EU.....	20
5.2 From Opt-out to Opt-in.....	20
5.3 The Introduction of EU Directive 2002/58/EC.....	21

Chapter 6 The Result of OECD on Spam and International Cooperation-The London Action Plan.....	23
6.1 Redefine the Contents of Spam.....	23
6.2 Set Anti-spam Regulation.....	24
6.3 Spam Issue in Developing Countries.....	24
6.4 Action required by the Developing Countries.....	25
6.5 International Cooperation-The London Action Plan.....	27
 Chapter 7 The Spam Solution of Taiwan.....	 28
7.1 Current Law and Regulations in Taiwan.....	28
7.2 Freedom of Speech.....	29
7.3 The History of Legislation on Spam.....	30
7.4 Competent Authority.....	31
7.5 Contents of the Draft Act.....	31
 Chapter 8 Conclusion.....	 33
8.1 International.....	33
8.2 Taiwan.....	34



Preface

This Article is divided into three parts. Part one is an introduction of spam, explaining the problems caused by spam, who profits from spam, and how spammers collect email addresses. Moreover, it contains some cases to analyze the conflicts between freedom of speech and privacy. Part two quickly sketches the three-part responses to spam by Internet Service Providers (“ISPs”) and businesses: self-regulation, technological innovation, and legislation. Additionally, developments in recent litigations will also be included. Part three will introduce EU’s attitude towards spam and its opt-in rule. Furthermore, I will address the consequences of the Organization for Economic Cooperation and Development (“OECD”) on spam. Part three will discuss and analyze whether it is necessary to enact an exclusive law on spam in Taiwan.

Chapter 1 The Problem of Unsolicited Commercial Emails

1.1 The Problem of Unsolicited Commercial Emails

Every morning, when you access to your e-mail account, an uncomfortable feeling arises because you get a bulk of unsolicited commercial emails and most of them are pornographic or obscene. “You’ve Got a Mail” no longer seems romantic to the Internet users.

According to a recent survey reported by the Consumer’s Foundation¹, 95% of the Internet users access the Internet every day, 93% of these users receive unsolicited commercial emails every day and usually they get an average of 100 unsolicited commercial emails. Moreover, this research indicates that Taiwan’s Internet users have to spend 30 hours per year in deleting these e-mails if we estimate the deletion of a commercial e-mail only takes 3 seconds. Additionally, 87% of unsolicited commercial emails are pornographic and cause a lot of teenagers to be exposed to these pornographic commercial emails. From this research, the unwilling receipt of these commercial emails makes the Internet Users more aggravated.

1.2 What is Spam?

¹只要郵件，不要垃圾！還給消費者一個清淨的網路環境！, The Consumer Function, Chinese Taipei at <http://www.consumers.org.tw/unit412.aspx?id=553>, last visited on February 28,2007.

Though “unsolicited commercial email” is a legal term, people usually call this unsolicited commercial email “spam” or “junk email”. The term “spam” was not so popular in the early 1990s, referring to annoying and distracting cross-postings among Usenet discussion groups.² In 1970, a famous TV commercial featured a Viking troop singing in the background, spam, spam, spam, spam.³ Thus, Usenet denizens identified any mass Usenet posting that interfered with their discussions as “spam”. Now, this term is identified as unsolicited commercial email (“UCE”) or unwanted unsolicited bulk e-mail (“UBE”)⁴.

1.3 A Fast, Convenient and Effective Marketing Tool

Who profits from spam? The companies that utilize commercial email as a direct marketing tool have found it to be one of the most cost-effective ways to advertise. With a “click”, email can reach millions of consumers at a modest cost and on a global level. Besides, some software companies that create anti-spamming programs and technology⁵ also make a fortune from poor Internet users.

Who bears the cost of spam? First, the recipient of spam is required to pay for additional time of Internet access in order to download, delete and register complaints against the unwanted solicitation emails. Microsoft did some research on spam.⁶ It found that 93% of the interviewees are disgusted with spam, 76% of the Internet users delete spam without reading it and 73% of Internet users asserted that they could claim damages against spam and spammers for criminal behavior.

Second, ISPs bears the cost when transmitting spam. Additionally, ISPs must deal with the problem of increasing bandwidth, requiring the expenses in large amount on hardware to accommodate the increasing volume of email sent and stored on a daily basis. Taiwan ISPs calculated that the cost of transmitting one spam was NTD 0.02, and it cost them about NTD 3-3.5

² See The Jargon Files, at <http://www.houghi.org/jargon/spam.php>, last visited on 28 Feb. 2007.

³ See SPAM and the Internet, at http://www.spam.com/ci/ci_in.tm, last visited on 28 Feb.2007.

⁴ Gray J.Fechter and Margarita Wallach, Spamming and other advertising issues: banner and pop-ups, ALI-ABA course of study materials, April 2005.

⁵ Id.

⁶ Id.

million per year.⁷ Unfortunately, the increasing expenses incurred by the ISPs are transferred to the consumers in the form of more hourly and monthly charges.⁸

1.4 How Can Spammers Acquire Your Email Accounts and Private Information?

If you have an email address, you will undoubtedly receive spam. But the question is how spammer can get your email accounts and private information, such as your personal preferences, account numbers, or credit card numbers. There are several ways for spammer to collect such information:⁹

- (a) Users sign up for something on the Internet: Many web sites collect personal information through on-line registrations, mailing lists, surveys, user profiles, and order fulfillment requirements. According to a Federal Trade Commission (“FTC”) released report,¹⁰ ninety-two percent of commercial web sites collect personal information. Only 14 percent of the web sites provide notices with respect to their information practices and only two percent have a comprehensive privacy policy. Therefore, if you sign up for something on any commercial web site, you will probably disclose your email account to spammers.
- (b) Users have their emails disclosed on the Internet: Even if you do not sign up on the web site, your company’s web site may disclose your email account and personal information, such as telephone numbers or address for commercial contact. However, spammers could take advantage of this web site if they insert key words to search the target buyers.¹¹
- (c) Spammers send emails at random: Spammer does not collect any personal information, but use random selection of common email addresses at known domains. For example, a lot of Internet users use john@yahoo.com or marry@hotmail.com as their email addresses which are easily presumed by

⁷ 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

⁸ Legislative update: Regulating your Internet Diet: The Can SPAM Act of 1999, 10 DePaul-LCA J. Art& Ent. L. 175, Vasiliou Toliopoulos at 175,177. (1999)

⁹ Information technology Law: un-canned Spam: getting it back in the tin, Don Passenger and Jeff Kirkey, 82 MI Bar Journal (March, 2003)

¹⁰ See FTC web site at www.ftc.gov/opa/1998/06/privacy2.htm,last visited on November 30,2005.

¹¹ See Id. 6

spammers.

- (d) Spammers obtain malicious receipt of personal information: If spammers are skilled computer users, they can collect email addresses by directing users from a legitimate web site to a fraudulent copy of that site.¹² Some users are not aware of this bogus web site, and insert their identity including email address.

Chapter 2 Conflict with Freedom of Speech

Since ISPs and Internet users are unwilling to accept spams, could they use any methods to block these unsolicited commercial letters? First, we have to analyze whether these emails are protected by freedom of speech.

2.1 Freedom of Speech

The First Amendment provides that “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof or **abridging the freedom of speech...**”. Though the Constitution gives protection relating to freedom of speech, prior to 1976, “commercial” speech, such as advertising, was not protected under the First Amendment. In *Valentine v. Chrestensen*,¹³ the respondent owned a former United States Navy Submarine which he exhibited for profit. He prepared and printed a handbill advertising the boat and soliciting visitors for a stated admission fee. He was advised by the petitioner, the Police Commissioner, that this activity would violate 318 of the Sanitary Code which forbids distribution on the street of commercial and business advertisements.¹⁴ The Supreme Court held that the commercial speech should be governed and controlled by government under the police power. Thus, it seems that commercial speech is not under protection of freedom of speech.

However, absolute bans on advertising by businesses and professionals have also been struck down. In *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*,¹⁵ the court held that commercial speech

¹² Identity Thieves’ New Ploy: Pharming, San Jose Mercury News, Knight Ridder newspapers, Dan Lee (2005)

¹³ *Valentine v. Chrestensen*, 316 U.S. 52 (1942)

¹⁴ *Id.* at 53

¹⁵ *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980)

is “an expression related solely to the economic interests of the speaker and its audience.”¹⁶ Additionally, it established a four-part test to determine whether the commercial speech is under the protection of the First Amendment:

- (1) Whether the speech at issue concerns lawful activities and is not misleading;
- (2) Whether the asserted governmental interest is substantial;
- (3) Whether the regulation directly advances the governmental interest asserted, and;
- (4) Whether it is no more extensive than is necessary to serve that interest.

In *Bolger v. Youngs Drug Products Corp.*¹⁷, the appellee, Youngs Drug Products Corp (“Youngs”), was engaged in the manufacture, sale, and distribution of contraceptives. The appellee used the various methods to publicize the availability and desirability of its products. One of the methods was to send unsolicited mass mailings to the public. The Postal Service thought that these unsolicited mailings violated 39 U.S.C. § 3001 (e)(2) stating that any unsolicited advertisement which is designed, adapted, or intended for preventing conception is nonmailable matter. The appellee argued that the above statute could not constitutionally restrict its mailings. The appellate court held that the Young’s mailings were not false, deceptive or misleading and was entitled to the First Amendment’s protection. Moreover, such restriction of contraceptive mailings is more extensive than the Constitution permits.¹⁸

The above cases are limited to traditional commercial speech. In 2005, in *White Buffalo Ventures, LLC v. University of Texas*, the United States Court of Appeals for the Fifth Circuit adopted the Central Huston four-part test.¹⁹ In this case, the plaintiff, White Buffalo Ventures LLC (“White Buffalo”), sent its unsolicited emails to the email account holders of University of Texas at Austin (“UT”). Pursuant to UT’s international anti-solicitation policy, the defendant UT blocked White Buffalo’s attempts to send unsolicited bulk commercial letters. White Buffalo filed an injunction against UT excluding its incoming emails.²⁰ However, the district court denied the motion for

¹⁶ *Id.* at 561.

¹⁷ *Bolger v. Youngs Drug Products Corp.*, 463 U.S. 60,62 (1983).

¹⁸ *Id.* at 73.

¹⁹ *White Buffalo Ventures, LLC v. University of Texas at Austin*, 4F.3d 366, 368 (2005).

²⁰ *Id.* at 372.

injunction. Then, White Buffalo appealed, challenging that the policy of UT violated the First Amendment. The appellate court did not dispute the commercial character of White Buffalo's emails. Then, the appellate court analyzed the legality of UT's policy under the four-part test. First, both parties agreed that White Buffalo's commercial emails were legal and contained accurate information (the first prong). Besides, UT's policy was a more direct means of preventing commercial spam from appearing in the account-holder's boxes (the third prong). Moreover, the policy was narrowly and specifically drawn to protect the system and users from those unsolicited, commercial emails identified as problematic (the fourth prong). Finally, though the government did not admit any protection of UT's interest, the policy met other protected interest, i.e., user efficiency interest (the second prong).²¹

Through transformation of the concept of the First Amendment, commercial speech is under protection of freedom of speech. The government shall measure the balance of substantial interest and freedom of speech when enacting any restrictions.



2.2 Pornographic /Obscene Speech

If the commercial speech contains pornography / obscene materials, shall such speech be protected under the First Amendment? The Federal Circuit Court opined that pornographic /obscene speech is lack of social importance; therefore, such speech is not entitled to protection under the First Amendment. But is there any clear definition of “obscene”? In the Miller v. California case, the Supreme Court held that to be obscene, the work, taken as a whole, must be judged by “the average person applying contemporary community standards” to appeal to the “prurient interest” or to depict “in a patently offensive way, sexual conduct specifically defined by applicable state law” and lack “serious literary, artistic, political or scientific value”.²²

As to pornographic materials involving minors, the Supreme Court held that

²¹ *Id.* at 374-376.

²² *Miller v. California*, 413 U.S. 15 (1973).

any picture containing sexual behavior of minors or sexual organs is not protected by freedom of speech even if it does not meet the definition of obscene speech. The government should be able to strictly limit the dissemination and communication of such materials.²³

Chapter 3 Three-step Responses to Spam

Since the Internet consists of Internet Protocols (“IP”) from different computers, the transmission of information from one computer’s IP to another computer’s IP, the identity of sender, recipient and even user are anonymous. Anonymity attracts users and creates business opportunities, but also brings disadvantages to its users.

There are three steps that may block spam:

3.1 Self-regulation

(1) Self- regulation concerning collecting email addresses: A frequent way to reject this spam is **Not** to disclose your personal information through online registrations, surveys and forms. The web site that you log on to should tell you about its security, encryption and policy related to spam. The Internet users have the right to deny their collection.

However, it is hard to achieve self-regulation due to personal factors. According to the Electronic Privacy Information Center’s Survey,²⁴ in which the Center surveyed the Top 100 web sites and examined their privacy on the Internet, many web sites collect personal information through on-line registrations, mailing lists, surveys, user profiles, and order fulfilling requirements. The Center only found 17 of the sites actually had privacy policies, and few were easy to find, not to mention whether users could restrict the secondary use of their personal information. Therefore, self-regulation is not an effective method to solve the problems.

²³ Paris Adult Theatre I et al. v. Slaton, 413 U.S. 49 (1973).

²⁴ Surfer Beware: personal privacy and the internet, electronic privacy information center. (1997), see www.epic.org/reports/surfer-beware.html , last visited on November 30,2005.

3.2 Technological Innovation

Recently, ISPs and businesses have spent money and time in filtering out spam. There are several ways for them to defend against this:²⁵

3.2.1 Blackhole List: this consists of a list of email accounts. Any email coming from the email account which is listed in the blackhole will be blocked by the mail server. However, this technology is not perfect. Sometimes, it will not be able to block spam which is not listed in the blackhole, and some legitimate and important mails will never reach their destinations. To overcome these defects, the blackhole list is replaced by a whitehole list. The whitehole list allows emails to pass through if they are listed on the list. Notwithstanding, the whitehole list also has the same defects as the blackhole list, some normal emails can not reach their destinations.

3.2.2 Keyword Filtering: another way to block spam is that email administrators take time and effort to set up a keyword list. If one of the keywords is shown in the content of the email, this email will be filtered out and a notice will be sent to the email administrator. Though it seems to be an efficient way to control the quality of emails, server administrators and users have to inspect and modify keywords to keep the filtering quality in good order from time to time.

3.2.3 Filtering by experience: according to lengthy experience in defeating spam, email administrators and mail servers can tell spam from legitimate emails by the size of the email, fraudulent email addresses, mails with special HTML tags, and so on. For example, if there are inconsistencies in email addresses in the SMTP mail form and the form in the email content, this email will be highly regarded as spam.

3.2.4 Email account application control: to avoid becoming senders of spam, some ISPs require their applicants to fill in their names and phone numbers for control.

²⁵ 垃圾郵件處理常見問答問題四，see www.openfind.com.tw/act/mail2000/security/faq.htm, last visited on December 16, 2005.

3.2.5 Spam complaints set up: recipients forward spam to ISPs and ISPs will develop spam recognition technology by anglicizing millions of these mails.

The ISPs and tech support departments of companies constantly use the above methods to block spam, but unfortunately, spammers steadily work on circumventing these efforts. AOL representatives characterize their efforts at filtering spam as “a cat and mouse game” between AOL and spammers.²⁶

3.3 Legislation

Early on, there were no special laws to block spam; therefore, some courts tried to solve the spam issue by using traditional tort theories such as trespass or nuisance:

3.3.1 Trespass to Chattel

The courts used the doctrine of trespass to chattel when dealing with spam cases in the early stage. Though ISPs and businesses had won in court battles against spammers for several years,²⁷ using the doctrine of trespass to chattel, these rulings exposed a fundamental flaw in the litigation strategy against spammers, i.e. the legal wrong of spammers. Since the doctrine of trespass to chattel requires an injury proximately caused by the alleged tortfeasor's interference with the **possession** of the plaintiff's chattel,²⁸ yet ISPs and businesses suffered only indirect and consequential harm from spam, such as the cost of redeploying tech support personnel to block emails and the projected losses in employee productivity resulting from the time spent reading or deleting spam.²⁹ In *Intel Corp. v. Hamidi*, the California Supreme Court clearly reasoned that reading emails transmitted from equipment designed to receive them, in and of itself, does not affect the possessory interest in the equipment.³⁰ It seems that common law is insufficient to solve

²⁶ Adam Mossoff, *Spam-Oy, It's such a Nuisance* (2004).

²⁷ see *America Online Inc. v. LGM, INC.*, 46 F. Supp.2d 444 (E.D. Va. 1998); *America Online, Inc. v. IMS*, 24 F.Supp.2d 548 (E.D. VA. 1998); *Hotmail Corp. v. Van\$ Money Pie, Inc.*, 1998 WL 288289 (N.D. Cal. 1998); *Compuserve Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997); eBay also successfully used trespass to chattel to sue an Internet company that was searching eBay's auction without authorization, see *eBay Inc. v. Bidder's Edge, Inc.*, 200 F. Supp.2d 1058 (N.D. Calif.2000).

²⁸ *Intel Corp. v. Hamidi*, 30 Cal.4th 1342,1348 (2003).

²⁹ *Id.* at 1349 & 1352-53 (noting that Intel submitted uncontroverted evidence that employees requested that the email be blocked and that Intel's technical support staff spent “time and effort” in attempting to block the emails.

³⁰ *Id.* at 1359 (quoting *Intel Corp. v. Hamidi*, 94 Cal.App.4th 325(2001) Kolkey, J., dissenting).

spam problems.

3.3.2 Nuisance

The difference between trespass and nuisance is as follows: “If the intrusion interferes with the right to exclusive possession of property, the law of trespass applies. If the intrusion is interfered with the interest in the use and enjoyment, the law of nuisance applies.”³¹ ISPs and businesses suffer substantial injuries arising from interference with the use and enjoyment of their property. In *Parker v. C.N. Enterprises Order*,³² the court held that defendants did not and do not have the legal right to use plaintiffs’ email addresses as a return address for their mass mailing, and the defendants’ unauthorized use of that address constituted a common law nuisance. However, this doctrine applies only to certain types of spammers.

3.3.3 Introduction of State Laws

Several years ago, anti-spam advocates had lobbied the U.S. Congress to pass laws regulating spam. However, Congress did not pass national legislation at that time since marketing industry had more powers. Consequently, 19 state legislatures have enacted their anti-spam acts since 1998.³³

The first state to enact its law was Washington, and then came California, Illinois and Virginia.

There are several mechanisms used by these states to prohibit spamming:

- (a) Truth-in-labeling principle: some state laws (California’s statute is the leading example) require spammers to use the label “ADV:” in their subject headings. Moreover, some states require that spammers who send adult materials use the label “ADV: ADLT: ” in their subject headings.
- (b) Opt-out choice: state laws require spammers to give recipients an opt-out choice. If the recipients are unwilling to receive further emails, they can inform senders through such opt-out choice.
- (c) Actual mailing address: spammers should provide an actual mailing

³¹ see *Exxon Corp. v. Yarema*, 69 Md. App. 124,148 (1986).

³² *Parker v. C.N. Enterprises Order* in the district court of Travis County, Texas 345th Judicial District (No.97-06273).

³³ Douglas J. Wood, *The Impact of State Anti-Spam Laws* at www.gigalaw.com, last visited Dec, 14, 2005.

address.

- (d) General principle: unlike the truth-in-labeling principle, some states (Washington’s statute is the prime example) require spammers to use the general language in the message header.
- (e) Right of the ISP: some states allow ISPs to sue spammers for damages.
- (f) Right of the recipient: a number of states grant individuals the right to sue spammers for damages.³⁴

List of State Anti-Spam Laws

State	
California	Labeling/Opt-Out
Colorado	Labeling/Opt-Out
Connecticut	General
Delaware	General
Idaho	Accurate Mailing Address/ Opt-Out
Iowa	Accurate Mailing Address/Opt-Out
Louisiana	Accurate Mailing Address
Missouri	Opt-Out
Nevada	Labeling/Opt-Out
North Carolina	Accurate Mailing Address
Oklahoma	Accurate Mailing Address
Pennsylvania	Labeling (Adult Materials Only)
Rhode island	Accurate Mailing Address
Tennessee	Labeling/Opt-Our
Virginia	Accurate Mailing Address
Washington	General
West Virginia	General
Wisconsin	Labeling (Adult Materials Only)

Source: This list was originally published at GigaLaw.com on March 2002.

Chapter 4 The CAN –SPAM Act

4.1 History

The U.S. Congress finally passed “anti-spam” legislation in December 2003.

³⁴ Id.

One Act, entitled “Controlling the Assault of Non-Solicited Pornography and Marketing Act”³⁵(The Can-SPAM Act), became effective on January 1, 2004. It intends to create one national standard of spam regulation and is applied not only to the person or entity sending the commercial email message but also to the person or entity advertising through such message. The CAN-SPAM Act preempts state laws that expressly regulate the use of email to send commercial messages, except to the extent that such laws prohibit transmission of false or deceptive email messages.³⁶

4.2 The Definition of Commercial Electronic Mail Messages

The definition of commercial electronic mail messages is limited. The CAN-SPAM Act separates transactional or relationship messages from commercial electronic mail messages. The purpose of the former is to confirm previously agreed transactions, provide warranty information, change notification, or deliver goods or services. The latter, under the section 3 of the CAN-SPAM Act, refer to any electronic mail message whose primary purpose is the commercial advertisement or promotion of a commercial product or service.³⁷ Though transactional or relationship messages are excluded from the broad definition of commercial email messages,³⁸ the commission can modify the definition of messages to accommodate changes in electronic mail technology or practices.³⁹

4.3 Relevant Regulations

According to The CAN-SPAM ACT, email senders shall not use false or fraudulent header information with a from line to identify a person initiating

³⁵ The “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003” was signed on December 16, 2003, by President George W. Bush. The Act will be codified at 18 U.S.C. 1037.

³⁶ Cooley Alert ,The CAN-SPAM Act: How it Affects You, Cooley Godward LLP (2004).

³⁷ 15 U.S.C. 7702 (2) (A)

³⁸ 15 U.S.C. 7702 (17) (A) (i)-(v): (i) to facilitate, complete, or confirm a previously agreed upon commercial transaction, (ii) to provide warranty, product recall, or product safety or security information with respect to a commercial product or service used or purchased by the recipient, (iii) to provide notification concerning a change in terms or features, notification of a change in recipient’s standing or status, account balance information, or any type of account statement with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship. (iv) to provide information directly related to an employment relationship or employee benefit plan in which the recipient is participating; or (v) to deliver goods or services (including upgrades) that the recipient is entitled to receive under the terms of a prior transaction.

³⁹ 15 U.S.C. (17) (B)

the message.⁴⁰ Besides, email senders shall conspicuously and clearly give recipients an opportunity to turn down future email from the senders, and provide a reply in the manner specified in the email, a reply email address or Internet-linked page for the recipients' use.⁴¹ Such mechanism shall remain operating within no less than 30 days after transmission of the original message. When receiving a recipient's reply, the email sender shall not transmit other emails to the recipient within 10 business days after receiving such request.⁴²

Additionally, the CAN-SPAM Act also provides that the sender shall conspicuously and clearly identify whether the message is an advertisement or solicitation⁴³ and provides a valid physical postal address of the sender.⁴⁴ The sender is prohibited from using scripts or other automated means to register multiple email accounts or online user accounts from which messages are intended to be transmitted to a protected computer.⁴⁵ Moreover, if the sender initiates transmission of any email message that includes sexually oriented material, the sender shall mark the email subject heading in the manner prescribed by the Fair Trade Commission.⁴⁶

	Commercial E-Mail Messages	Transactional or Relationship E-Mail Message
False Header Information	Prohibited	Prohibited
Misleading Subject Line	Prohibited	Not Addressed
Opt-Out Notice	Required	Not Required
Identification as Advertisement	Required	Not Required
Valid Physical Postal Address	Required	Not Required
Warning for	Required	Not Required

⁴⁰ 15 U.S.C. 7704 (a)(1)(A), (B) and (C).

⁴¹ 15 U.S.C. 7704 (a)(3)(A).

⁴² 15 U.S.C. 7704 (a)(4)(A).

⁴³ 15 U.S.C. 7704(a)(5)(i) .

⁴⁴ 15 U.S.C. 7704(a)(5)(iii) .

⁴⁵ 15 U.S.C. 7704 (b)(2).

⁴⁶ 15 U.S.C. 7706 (a)(1).

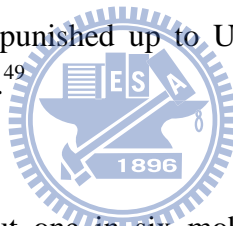
Sexually Oriented Material		
----------------------------------	--	--

Source: Technology Commentaries: the Federal CAN-SPAM Act-New Requirements for Commercial E-mail.

4.4 Law Suits and Damages

Who can bring suits against spammers? The Act empowers a number of federal agencies, including the FTC, to bring forth enforcement actions.⁴⁷ States and ISPs may, with certain exceptions, sue violators of the CAN-SPAM Act.⁴⁸ However, the recipient does not have any right to claim damages against spammers, but he/she can initiate state-law-based “spam” suits.

Under the CAN-SPAM Act, each separately addressed unlawful message received by or addressed to such residents is treated as a separate violation. Each violation may be punished up to US\$250 with the total amount not exceeding US\$2000,000.⁴⁹



4.5 Mobile Spam

In the United States, about one in six mobile phone users report receiving unsolicited text messages on their phones from advertisers. Although every major wireless company has spam filters and other methods to block spam, the U.S.A. subscribers will receive about 1 billion text-based spam messages in 2007.⁵⁰

Mobile service commercial messages (MSCMs) are defined as those “transmitted directly to a wireless device that is utilized by a subscriber of a commercial mobile service.....in connection with that service” under Article 13 of the CAN-SPAM Act.⁵¹ The Act makes it clear that Congress specifically contemplated restrictions on email messages.⁵² In addition, The CAN-SPAM

⁴⁷ 15 U.S.C. 7706(a)(1).

⁴⁸ 15 U.S.C. 7706(f).

⁴⁹ 15 U.S.C.7706(f)(3).

⁵⁰ Billing World & OSS Today Magazine at <http://www.billingworld.com/rev2/main/featureArticle.cfm?featureID=7843>, last visited on May, 5,2007

⁵¹ 15 U.S.C. 7712

⁵² Grappling with mobile spam at

Act requires the Federal Communication Commission (“FCC”) to promulgate rules governing the use of wireless email devices and mobile service by September 26, 2004. The FCC adopted rules that prohibit sending unwanted commercial email messages to wireless devices without prior permission, which took effect in March 2005. The FCC’s ban covers messages sent to cell phones and pagers, if the message uses an Internet address that includes an Internet domain name. Though FCC’s ban does not cover commercial messages from one mobile phone to another or from a computer to mobile phones, the Telephone Consumer Protection Act (“TCPA”) has restricted the use of telephone and fax machines from delivering unsolicited advertisements and has also established a “do not call list.”⁵³

4.6 Relevant Cases

After enacting of the CAN SPAM Act, the FTC and ISPs filed several cases against spammers. Here are some relevant cases:

4.6.1 Robert Braver v. Robert Soloway, et al.⁵⁴

Plaintiff Rover H. Braver is an Oklahoma ISP owner who received a bulk of emails from the defendant, Soloway and his companies. The plaintiff brought the suit against Soloway in state court. The decision was based on Federal CAN SPAM Act and Oklahoma law (fraudulent use of electronic and Oklahoma Unsolicited Commercial electronic mail statute). Based on Braver’s having received Soloway’s spam on about 200 separate dates and that the spam violated two separate Oklahoma laws, the plaintiff won a \$10 million judgment.⁵⁵

4.6.2 FTC v. Cleverlink Trading Limited, et al.⁵⁶

In 2004, the defendant, Cleverlin Trading Limited, operated numerous

http://www.usatoday.com/tech/columnist/ericjsinrod/2004-04-08-sinrod_x.htm, last visited on May 5, 2007

⁵³ Federal Communication Commission, at <http://www.fcc.gov/cgb/consumerfacts/canspam.html> last visited on May 10, 2007.

⁵⁴ Oklahoma Western U.S District Court-West District of Oklahoma civil docket for case: 5:05-cv-00210.

⁵⁵ Oklahoma Man wins \$ 10 million judgment against a spammer at http://www.circleid.com/posts/oklahoma_man_wins_10_million_judgment_against_a_spammer, last visited on March 5, 2007

⁵⁶ Spammer’s invitation to Date Lonely Housewives Halted by Court at FTC’s request at www.ftc.gov/opa/2005/05/housewives.htm, last visited on March 4, 2007.

websites containing sexually oriented materials. The commercial email messages directed consumers to the defendant's paid content web sites by containing hyperlinks that, when clicked, took consumers to the defendants' websites.⁵⁷ The FTC charged that the spam violated nearly every provision of the CAN-SPAM Act. It contained misleading headers and deceptive subject lines. It did not contain a link that allowed consumers to opt out of receiving future spam or disclose, as required by law, that it was sexually explicit. The FTC complaint was filed with the U.S. District Court for the Northern District of Illinois, Eastern Division, in Chicago. The Judge ordered a temporary halt to the spamming and froze the assets of the defendant.

4.6.3 Verizon Case

Defendants sent nearly 100,000 unsolicited text messages to Verizon wireless customers. The messages notified them to claim a Bahamas cruise they supposedly won. Plaintiff Verizon Wireless filed a case against Passport Holidays in the U.S. District Court in Trenton, N.J. Verizon accused Passport Holidays of sending unsolicited messages to its users and charged the text messages violated the FTCP. In the process of the litigation, Passport Holidays stated that the spam was actually sent by Marketing LLC and Specialized Programming. Based on this statement, Verizon Wireless filed an amended complaint in which it named Marketing LLC and Specialized Programming as defendants. In 2007, the Court ruled that the defendants must pay Verizon Wireless more than US\$ 200,000 and barred their further contact with Verizon Wireless' consumers.⁵⁸

4.7 The Enforceability of National Do Not Registry

The FTC submitted a report relating to false claims of SPAM pursuant to section 9 of the CAN-SPAM Act on April 30, 2003.⁵⁹ After that, the FTC submitted another report on National Do Not Email Registry Plan to Congress in June 2004.⁶⁰

⁵⁷ FTC v. Cleverlink Trading Limited et al, United States District court for the Northern District of Illinois Eastern Division, Case no. 0502889.

⁵⁸ <http://www.sophos.com/pressoffice/news/articles/2007/02/textspam.html>

⁵⁹ False Claims in Spam, a reported by the FTC's Division of Marketing Practices, April 30, 2003.

⁶⁰ National Do Not Email Registry A Report to Congress, Federal Trade Commission, June 2004.

4.7.1 False Claims in Spam

The FTC reviewed approximately 1,000 pieces of unsolicited commercial emails from July 2002 to Oct. 2002. The messages reviewed by FTC consisted of random samples from three FTC data sets: spam forwarded to FTC by the public (approximately 450 pieces), messages received by undercover FTC email boxes (approximately 450 pieces) and spam received by FTC employees in their official inboxes (approximately 1,000 pieces).⁶¹

The FTC analyzed false claims appearing in “From” and “Subject” lines as well as in the body of the messages. Investment/business opportunities, adult and finance offers comprised 55% of the types of offers being made in spam analyzed by FTC. Nearly 33% of the Spam contained false information in the “From” line. Of the messages containing indicators of falsity in the “From” line, nearly half claimed to be from someone with a personal relationship with the recipient.⁶² As to “subject” line, 22% of the spam contained false information in order to lure consumers into opening the message to see the contents related to the representations in the “subject” line. Though false “Subject” lines are found in all types of offers, over one-third of adult offers appear to misrepresent the contents of the message.⁶³ Moreover, over half of finance-related spam contained false “From” or “Subject” lines.

The FTC analyzed the falsity in the message text and found approximately 40% of the message had at least one indication of falsity. 90% of spam advertising investments and business opportunities contained signs of falsity.⁶⁴ 66% of spam contained false “From” lines, “Subject” lines or message texts. Moreover, 96 % of spam concerning investments and business opportunities contained false “From” lines, “Subject” lines or message texts.⁶⁵

Since then several states have enacted laws in recent years requiring senders of spam to begin every subject line with the phrase “ADV” in messages sent to recipients of those states. The FTC found that only 2% of spam complied with the rules. 17% of spam advertising pornographic websites contained

⁶¹ Supra 53 at 1

⁶² Supra 53 at 4

⁶³ Supra 53 at 6

⁶⁴ Supra 53 at 9

⁶⁵ Supra 53 at 10

“adult images” in the body of the message and 41% of spam contained false information in their “From” or “Subject” lines.⁶⁶

4.8 The Do Not Email Registry Report

The FTC worries that the current email system enables spammers to hide their tracks, and that spammers use many techniques to hide, including spoofing, open relays, open proxies, and zombie drones, which make it difficult to identify spammers through email headers and impede law enforcement.⁶⁷ In order to solve these problems, the FTC has proposed an authentication system to identify the origin of email messages. Additionally, ISPs also have tried to develop a system.⁶⁸

The FTC solicited models from the public to enforce the National Do Not Email Registry. Now, there are three possible ways to enforce this Registry: (1) Registry of individual email addresses (2) permitting ISPs and other domain holders to register their objection to receiving spam addressed to any email addresses located at their domains and (3) Registry of individual email addresses with a third-party forwarding service.⁶⁹

However, a National Do Not Email Registry containing individual email addresses could suffer from a significant security weakness that would enable spammers to treat the Registry as National Do Spam Registry. It could be a risk if spammers use the Registry to determine valid email addresses. The Consumers Union has stated that if the Commission were to adopt an individual email address Registry and distribute the Registry to marketers, the consumers would not sign up for it for security concerns.⁷⁰

The FTC has pursued a vigorous law enforcement program against deceptive spam, and to date has filed 62 cases, in which spam was alleged to be responsible for overall deceptive or unfair practice. The FTC experiences in these cases show that the primary law enforcement challenge is locating and identifying the targeted spammer. The FTC and ISPs can only trace spammers by tracing the flow of funds from victims to spammers. However,

⁶⁶ Supra 53 at 13

⁶⁷ Supra 54 at 8

⁶⁸ Supra 54 at 14-15

⁶⁹ Supra 54 at 15

⁷⁰ Supra 54 at 15-16

all of spammers, such are purely malicious for viruses. A prosecutor in Washington State spent four months and sent out 14 per-suit civil investigation demands (CIDS) to identify the spammer in one case⁷¹. Similarly, a Virginia attorney spent four months subpoenaing many witnesses before having enough information to file a case against a spammer.⁷²

ISPs have experienced similar obstacles in bringing suits against spammers. ISPs estimated that they expend an average of 133 hours per spammer.

4.9 Conclusion

The U.S has tried to fight against spammer in all ways it can. However, the law enforcement is not effective as expected. In my opinion,

- (a) Many spammers have moved their bases to other countries after the enactment of the CAN- SPAM Act, therefore; avoiding regulation under the CAN SPAM Act.
- (b) The purpose of adopting the National Do Not Email Registry is good, but if we can not develop an effective way to trace spammers, they may use the lists and send commercial emails to consumers. Such registry is criticized by FTC's report above and many scholars.
- (c) It is easier to trace outsourcing companies than spammers, therefore; through the enforcement, it is more possible to punish outsourcing companies than spammers.
- (d) Since the U.S. adopted the opt-out system, spammers can continue sending commercial emails without explicit rejection. Compared with the opt-in system adopted by the EU, it is relatively less effective.
- (e) In order to regulate spam effectively, the context of the CAN- SPAM Act should not only pertain to commercial emails but also include political or religious emails.
- (f) Private people cannot bring suits against spammers under the CAN- SPAM Act, so they have to use state law to claim damages. However, because the state laws vary, a private person usually is not aware of his/her rights under the state law.

Chapter 5 The Spam Solution of EU

⁷¹ WAOAG: Selis, 15. The Commission's spam cases routinely require the issuance of numerous CIDS.

⁷² VAOAG: Mcguire, 5-11

5.1 The Attitude of the EU

The reason why the EU tries to regulate spam is that it affects the fundamental rights of individuals. Spammers not only receive personal information and email account addresses illegally but also make it impossible for individuals to control the flow of information into their inboxes.⁷³ Moreover, spam transmits pornography and viruses via the Internet.

The EU is aware that only laws are not enough to solve the spam problem. Spam may be regulated through the cooperation of jurisdiction and technology. Therefore, EU law aims at two objectives: to reduce the amount of spam and guarantee the individual's control over personal information and contacts.⁷⁴

5.2 From opt-out to opt-in

The early thinking of the EU was to protect their citizens and consumers from “high-pressure selling methods”⁷⁵ and “certain particularly intrusive means of communication.”⁷⁶ So, regulating spam is governed by some Directives, which are not special for electronic communication.

Though EU Directive 95/46/EC (Framework Data Protection Directive) is not special for electronic communication, some provisions regarding the processing of personal information consider email addresses as personal data.⁷⁷ Therefore, the Directive applies to the processing of emails. Among other things, freely given, informed, specific and unambiguous consent must be provided by the addressee before the address is collected.⁷⁸ Collectors of email addresses must specify the explicit and legitimate collection purpose.⁷⁹ If someone collects email addresses from public Internet places such as websites, chat rooms, newsgroups and so on, he/she has violated the above Directive.

The above Directive indirectly protects the use of email accounts. EU

⁷³ European Union vs. Spam: A legal response, Nicola Lugaresi. Trento University, Law School.

⁷⁴ Id. at 1.

⁷⁵ Recital 5, Dir. 97/7/EC.

⁷⁶ Recital 17, Dir. 97/7/EC.

⁷⁷ Article 2 (a), Dir 95/46/EC.

⁷⁸ Article 2(a) and 2(h), Dir. 95/46/EC.

⁷⁹ Article 6(b), 10 and 11, Dir. 95/46/EC.

Directive 97/7/EC (Distance Contracts Directive) tries to regulate the transmission of emails. However, unlike transmission by automated calling systems and facsimile machines, which requires prior consent of the receiver,⁸⁰ the transmission of other communication such as email can be used without clear objection of consumers.⁸¹ The Directive does not define the meaning of “clear objection”.

Similarly, Directive 97/66/EC (Telecommunication Sector Privacy Directive) confirms the opt-in rule only with regard to automated calling systems or fax machines for the purposes of direct marketing.⁸² After that, EU Directive 2000/31/EC (Electronic Commerce Directive) confirms that member states could adopt the opt-in system for unsolicited commercial communications by electronic mail.⁸³ Finally, Directive 2002/58/EC (Electronic Communications Privacy Directive) confirms that prior consent given by consumers is required when sending unsolicited commercial email.⁸⁴

5.3 The Introduction of EU Directive 2002/58/EC (Electronic Communications Privacy Directive)

Article 13 of EU Directive 2002/58/EC (“Directive 2002”) defines spam as “electronic mail for the purposes of direct marketing.”⁸⁵ The term “electronic mail” covers any electronic communication including email, SMS, MMS and so on.⁸⁶ Since the 2002 Directive does not define “SPAM” as bulk of unsolicited commercial emails, sending one commercial email for marketing purpose could be deemed as “SPAM” under Article 13 of the 2002 Directive.

As we know, it is illegal to send commercial emails to consumers without their prior consent if we adopt the opt-in system. However, there are some provisions that may be exempted from this prohibition. For example, senders may send to the same email account information regarding similar products or services.⁸⁷ Nevertheless, recipients still should be given the

⁸⁰ Article 10 (1), Dir. 97/7/EC.

⁸¹ Article 10 (2), Dir. 97/7/EC.

⁸² Article 12 (1), Dir. 97/66/EC.

⁸³ Article 7(2) and recital 14, Dir. 2000/31/EC.

⁸⁴ DPWP, Opinion 7/2000, § 2, comment to article 3.

⁸⁵ Article 13, Dir. 2002/31/EC.

⁸⁶ DPWP, Opinion 5/2004, §3.1..

⁸⁷ Article 13 (2), Dir/ 2002/58/EC.

opportunity to object to the emails, as they are given in the opt-out system.⁸⁸ An issue could occur if such an email account is provided by a company or a family. In this situation, the prior consent must be given by the representative, not the actual user.⁸⁹

Article 13 (4) of the 2002 Directive prohibits the practice of sending electronic mails by concealing the identity of the sender, or without a valid address where the recipient can exercise the opt-out system.⁹⁰ However, the opt-in system only applies to a natural person.⁹¹ Since Directive 2002 only requires that Member States must provide sufficient protection of a natural person from spam.⁹² The Member states are free to adopt the opt-in/ opt-out system for a legal person. Such distinction between natural and legal persons makes law enforcement more difficult. It's hard for senders to identify whether this email account belongs to a natural person or a legal person. A better way is to require Member States to comply with the opt-in system regardless of a natural person or legal person.

Directive 2002 also encourages the industry filtering initiatives, through email system arrangements that allow recipients to view the sender and subject line for an email and to delete messages without having to download the contents or attachments,⁹³ for example, with “ADV” label in the subject line.⁹⁴ It is noted that without prior consent from consumers, it will not be legal even by labeling “ADV”.

Like the Do Not Email Registry in United States, Opt-out registry is considered under Directive 2002, however; it also exposes the same risk of possibly of infringing on the registrant's privacy.

⁸⁸ Recital 41 Dir. 2002/58/EC.

⁸⁹ Article 2(k), Dir. 2002/21/EC.

⁹⁰ Article 13 (4), Dir. 2002/58/EC.

⁹¹ Article 13 (5), Dir. 2002/58/EC.

⁹² Id.

⁹³ Recital 20 Dir. 2002/31/EC.

⁹⁴ Article 7, Dir. 2000/31/EC.

Chapter 6 The Result of OECD on Spam and International Cooperation-The London Action Plan

Since every country tries to enact the relevant spam regulations, the OECD has put more emphasis on the spam issue gradually. The OECD held a meeting in October 2005. During this meeting, the OECD not only tried to establish a set of regulations to assist every country on the SPAM issue but also examined the existing spam regulations of every country. Moreover, the OECD wished to figure out a solution for cross-border cooperation on the spam issue.⁹⁵

6.1 Redefine the Contents of Spam

The definition of spam varies in different countries. Some countries focus on a particular messaging medium such as email. Some provide a technology-neutral approach that provides an overreaching statement of principles that is more broadly applicable. The OECD recognized that spam has some of the following characteristics:

- (a) Commercial: the majority of spam is sent in order to acquire a profit.
- (b) Bulk: A common perception of spam is that it is sent or received in bulk. Spamhaus, an international anti-spam advocate, has estimated that more than 80% of the world's spam originates from 200 spam organizations. From this estimation, it is not difficult to search the origin of spam.
- (c) Misleading, pornographic or criminal contents: there are obvious community and regulatory agency concerns with the illicit content of a considerable amount of spam including those that promote pornography, illegal online gambling services and get- rich- quick schemes. Such contents will affect the minor's physical and mental state. Therefore, many regulators criminalize this type of spam under the existing laws such as in the EU.

Given the above, the OECD recognizes that spam can be transmitted by email, instant messaging, SMS, MMS, VOIP and Bluetooth.⁹⁶

6.2 Set Anti-spam Regulation

⁹⁵ Task Force on SPAM. Anti-SPAM Regulation, Directorate for science, technology and industry committee on consumer policy, committee for information, computer and communication policy, Organization for Economic Co-operation and Development, Nov. 15, 2005.

⁹⁶ *Id.* at 5.

The OECD points out that legislation alone will not stop potential spammers from taking advantage of this marketing technique. Legislators must cooperate with certain effective filtering programs and ISPs to actively filter such undesirable content.

6.3 Spam Issue in Developing Countries

The OECD also notices that spam is a much more serious issue in developing countries than in OECD countries. ISPs and network providers in developing countries lack the capacity and resources (for example, purchasing authorized software) to deal with sudden surges of spam that occur from time to time and this often causes their mail servers to break down or function at a sub-optimal level. Similarly, end users including consumers and businesses also lack knowledge to take effective actions against spam.⁹⁷ The OECD has tried to estimate the cost of filtering spam borne by the ISPs. According to its research, Outblaze limited is a large Webmail provider based in Hong Kong and China, that has over 40 million users around the world. The costs presented below are for filtering spam on just one of their mail sever clusters:

- Bandwidth costs USD 600 per month.
- Bandwidth consumption for mail is 70MB.
- 80% of incoming mail will be rejected as spam.
- 15% of spam passes filters.
- Monthly bandwidth cost of spam is USD 6300.
- Monthly storage cost of spam is USD 5400.
- Monthly salary expenses for mail administrators is USD 75,000.
- The total amount of the above costs is almost 10 % of one ISP bill.⁹⁸

ISPs in developing economies like India, which has more bandwidth and adequate data centre facilities, may find themselves infested by spammer customers, not just local spammers, but also spammers from the U.S. and the EU who shift their bases to developing countries.

The reasons why the OECD concludes it is hard to integrate developing countries are below:

- (1) Inaccurate, outdated and incomplete “Whois”: Developing countries often

⁹⁷ Id. at 4.

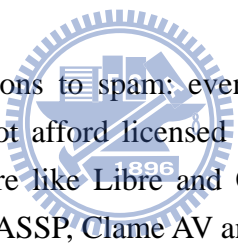
⁹⁸ Id. at 7.

have only one single ISP which provides Internet and email services to the entire country. This ISP does not modify the IP Whois records that it maintains in the RIR's Whois database nor does it maintain a publicly accessible "RWhois" database of IP assignments made to their customers. Therefore, smaller ISPs who buy bandwidth and lease IP addresses from this ISP only can be traced to the tier 1 ISP and no further. Consequently, the Tier 1 ISP becomes the de facto point of contact in the complaints about spam. Neither the Tier 1 ISP nor their customers have a dedicated team to deal with spam issues, and they do not even maintain postmaster or abuse account. Therefore, such spam issue solution will be delayed.

- (2) Pink contract: some ISPs will not reject spam if the spammer would like to pay more administration fees.

6.4 Action Required by the Developing Economies against Spam:

The OECD provides some solutions to assist the developing countries as follows:

- 
- (a) Technical solutions to spam: even though ISPs in the developing countries can not afford licensed filtering software, such ISPs can use free software like Libre and Open Source Software (FLOSS), Spamsassassin, ASSP, Clame AV and so on.
- (b) Formation of CSIRTs and CERTs: like Computer Security and Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs) help the developing countries to form an effective and efficient response to individual computer security incidents. Also, CSIRTs or CERTs may educate and train ISP personnel, systems and network administrators to develop the best security on computer.
- (c) Anti-spam policy setting and enforcement: ISPs must have a strong anti-spam policy and make it part of the "terms and conditions of the service" that a user must sign or agree with when he signs up for the ISP's service. ISP may reserve the right to terminate the contract and cease to provide service to a customer who violates any part of its anti-spam policy.

- (d) International co-operation: ISPs in the developing economies must integrate themselves with their peers in other economies if they attend NOG meetings or use the INOC DBA phone system-a closed VOIP phone network that directly connects different ISPs around the world. Therefore, ISPs in the developing economies can get more assistance.
- (e) Legislative and regulatory framework: Several countries have already called for the development of an international framework or signature of a Global MOU to fight spam. However, such framework will take a long time to complete. The developing countries may implement the relevant laws or regulations against spam or computer crimes along with adequate data protection. Moreover, the legislative measures must be backed by a well trained, sufficiently equipped and adequately funded enforcement arm.
- (f) Educating users: Teach users through media to understand what spam is and how to protect personal information and the way to fight spam.⁹⁹

Besides improvement of the developing countries, the OECD and the developed countries should provide some relevant assistance.

The OECD countries have already organized the Spam Task Force to put a “spam toolkit”, which exemplifies how to devise a spam law and refers to some existing structures. Australia signed MOUs with several countries to enable the countries to study and learn from its experience against spam. The FTC, together with UK Office of Fair Trading (OFT) has put forward the London Action Plan to exchange experiences in enforcement techniques and so on.¹⁰⁰

⁹⁹ Id. at 17-25.

¹⁰⁰ Id. at 28.

6.5 International Cooperation- The London Action Plan

6.5.1 Formation

On October 11, 2004, governments and public agencies from 27 countries met in London to discuss international spam enforcement cooperation. Based on the previous efforts of the OECD and OECD Spam Task Force and other international organizations,¹⁰¹ the participants issued this Action Plan.

The conference, hosted by the FTC and the United Kingdom's Office of Fair Trading,¹⁰² was the first international forum to address spam enforcement issues exclusively. There were 24 participants, including Taiwan.¹⁰³

6.5.2 The Content of the London Action Plan

The London Action Plan requires the members to (1) designate a contact window for further enforcement communication; (2) encourage communication and coordination among the different agencies and designate a contact for coordinating enforcement cooperation; (3) take part in periodic conferences to discuss (a) cases; (b) legislative and law enforcement developments; (c) effective investigative techniques and enforcement strategies; (d) the way to overcome the obstacles to effective enforcement; (e) how to train their consumers and businesses and (f) spam investigation techniques with representatives from private sectors; (4) encourage agencies and representatives from private sectors to fight spam; (5) prioritize cases based on international assistance; (6) complete the OECD Questionnaire on cross-border enforcement of anti-spam laws; and (7) encourage and support

¹⁰¹ Such as OECD, the international Telecommunication Union, the European Union, and the Asia-Pacific Economic Cooperative Forum.

¹⁰² FTC, International Agencies Adopt Action Plan on SPAM Enforcement, October 12, 2004

¹⁰³ Australia, Belgium, Canada, Chile, China, Denmark, Finland, Hungary, Ireland, Japan, Latvia, Lithuania, Malaysia, Mexico, Nigeria, Norway, republic of Korea, Spain, Sweden, Switzerland, Taiwan, The Netherlands, UK, USA. Agencies including Office of Fair Trading (UK), Information Commissioner Office (UK), Federal Trade Commission (US), Australian Communications Authority, Australian Competition and Consumer Commission, Dutch Telecommunications Regulator, Korean Information Security Agency, Ministry of Economic, Trade and Industry (MERI), Ministry of Internal Affairs and Communications (Japan), Japan Fair Trade Commission, Spanish Data Protection Agency, National Consumer Service (Chile), State Secretariat for Economic Affairs (Switzerland), General Inspectorate for Consumer Protection of Hungary, Finnish Consumer Agency and Ombudsman, Norwegian Consumer Ombudsman, Swedish Consumer Protection Agency, Data Protection Commissioner (Ireland) and Communications Regulatory Authority of the Republic of Lithuania.

the less developed countries in spam enforcement cooperation.¹⁰⁴

In order to begin the work pursuant to this Action Plan, the U.K. Office of Fair Trading and U.S. Federal Trade Commission will utilize their best efforts to (1) collect and disseminate information, including points of contact, notifications from new participants of their willingness to endorse this Action Plan; and responses to the questionnaire of the OECD; (2) set up conference calls and (3) provide a contact for further communications.¹⁰⁵

The Action provides members with information about increasing and decreasing spam and viruses monthly and submits an annual security report to its members. In its 2005 annual security report, it pointed out that spammers using phishing methods¹⁰⁶ to attract victims were a major threat during 2005.¹⁰⁷ The report predicted that 3G will become the target of spam through development of technology and communication.¹⁰⁸

Chapter 7 The Spam Solution of Taiwan

7.1 Current Law and Regulations in Taiwan

Since spam problems are arising now, we should examine some existing laws to solve spam problems:

7.1.1 Privacy protection: first, we shall discuss whether an email account constitutes a part of the user's personal information. According to Article 3 I (1) of the Computer-Processed Personal Data Protection Law ("CPPDP")¹⁰⁹, personal data mean any data that can serve to identify a specific person. Given that the email account is identifiable, it is regarded as personal data.

¹⁰⁴ The London Action Plan on Intentional Spam Cooperation Enforcement Cooperation at <http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf#search='london%20action%20plan>, last visited on March 21, 2007.

¹⁰⁵ *Id.*

¹⁰⁶ Spam appears as though it has originated from inside the organization. Often, the perpetrator will offer a small reward in return for information and individuals who are duped into thinking the emails are legitimate often comply.

¹⁰⁷ MessageLabs Intelligence 2005 Annual Security Report, at <http://www.londonactionplan.com/files/messagelabs/MLI%202005%20report%20Final.pdf>, last visited on March 22, 2007.

¹⁰⁸ *Id.* at 13.

¹⁰⁹ The terms used herein denote the following meanings: 1. Personal data: the name, date of birth, I.D. Card number, characters, fingerprints, marital, family, educational, occupational, and health status, medical history, financial conditions, social activities of a natural person and other data which can serve to identify the said specific person.

Any person who collects and uses such personal information without the owners' consent is punishable under criminal and administrative laws.¹¹⁰ However, CCPDP only applies to certain industries.¹¹¹ No violation of CCPDP will be constituted if other industries or persons collect, use or provide email accounts to third parties. Moreover, email accounts and transmission can be deemed as private. The court reasoned that if employees believe that they can reasonably expect the privacy on email transmission via computers owned by the employer, the email account can be deemed as private.¹¹² Therefore, if a third party disseminates emails through other persons' email accounts without the email users' consent, it is possible to violate the privacy right provided under the civil law.¹¹³ But this is only a theoretical reason, and the definition of reasonable expectation is so vague; therefore, it is not widely accepted in practice. As a result, there will be different views when judging whether an email account is private or not.

7.1.2 Misleading Advertisement: Under Article 21 of the Fair Trade Law ("FTL"), no enterprise shall make or use false or misleading representations or symbols as to price, quantity, quality, content, production process, or in any other way make known to the public. If the contents of an email are false or misleading representations, the email user can claim damages against the spammer in accordance with the FTL. Moreover, if any advertising agency makes or designs any advertisement that it knows or is able to know is misleading, it shall be jointly and severally liable for the damages to the principal of such advertisement under Article 21 of the FTL. However, FTC only regulates competition and enterprises. The FTL neither applies to natural persons nor regulates false and misleading headers, subjects, origins, and data from senders. The Consumer Protection Law also faces the same difficulties on limited subjects, i.e., enterprises.¹¹⁴

7.2 Freedom of Speech

According to Article 11 of the Constitution, people shall have freedom of speech, teaching, writing, and publication. Article 11 of the Constitution protects the freedom of active expression and passive omission of people.

¹¹⁰ Articles 33 and 38 of CPPDPL.

¹¹¹ Article 8 of CPPDPL.

¹¹² 91 Lao Su Tzu No.139.

¹¹³ Articles 18 and 195 of Civil Law.

¹¹⁴ Article 22 of the Consumer protection Law.

The scope of protection includes expressions of subjective opinions and statements of objective facts.¹¹⁵ Does freedom of speech, guaranteed by Article 11 of the Constitution, include commercial speeches made with the intent to obtain profits through sales of goods and concepts?

In theory, our country adopts “the two-level theory” with respect to freedom of speech, which means that speeches are not protected equally by the Constitution. The standard of scrutiny varies with the value of speech.¹¹⁶ In practice, under the Judicial Yuan Explanations Nos. 414 and 577, as a means to provide subjective information of a product, product labeling constitutes a type of commercial speech and shall fall within the scope of protection provided to speech by the Constitution. However, to advance other substantial public interests, the government may adopt some more restrictive means through legislation to serve government objectives by requiring product suppliers to provide material product information. Given the above, commercial contents are strictly regulated by competent authorities. As to pornography/obscene language or publications, it cannot be protected under freedom of speech. According to Judicial Yuan Explanations No. 407, the standard for judging whether a publication constitutes a crime of obscenity by instigating obscene conduct may vary because of differences in customs and ethics in various nations, but one thing in common among different nations is the governmental regulation of obscene publications. Obscene publications are those publications that, by objective standards, can stimulate or satisfy a prurient interest, generate among common people a feeling of shame or distaste, thereby offending their sense of sexual morality, and undermining societal cultural ethics.

7.3 The History of Legislation on Spam

In early June, 2002, forty people including legislator Feng Ting Kuo submitted the a draft for the Governing Commercial Electronic Mail Act. However, regrettably this draft is pending due to unfinished legislation processes after passing the first reading. Now, the Preliminary Office of the National Communications Commission, Administrative Yuan, has drafted the Governing Commercial Electronic Mail Abuse Act, and submitted the draft

¹¹⁵ Judicial Yuan Explanation No. 577.

¹¹⁶ He Hsiang Hung , Constitution Law , Published by La Sheng Co. , August, 2006

to the Legislative Yuan in Feb. 2005 for examination. After the 2nd meeting of 1st session of the 6th term held on March 21, 2005, the draft was processed together with the “Draft of Regulations Governing Spam” proposed by the Legislative Yuan in June 2002. Presently, the Legislative Yuan has delivered the draft to the Technology and Information Commission for examination after the first reading. On May 2, 2005, the administrative authority provided the legislative reasons and was prepared to be interrogated. A hearing for the “Draft of Regulations Governing Abusing Commercial Emails” (“Draft of Reg.”) will be held later.¹¹⁷

7.4 Competent Authority

In this Draft of Reg., the competent authority is the National Communications Commission (“NCC”). The reasons why the NCC was chosen is that NCC, as the competent authority of communication industries, has more strategies and incentives to actively assist ISPs in filtering spam. Besides, the competent authority has to highly interact with ISPs in the spirit of the Draft of Reg.; therefore, the NCC is the proper agency to deal with spam and relevant problems.

The main responsibilities of the NCC is to take relevant actions to ensure enforcement and amendment of Draft of Reg., promote ISPs to establish self-regulations, exchange anti-spam policies, encourage industries to develop techniques for anti-spam solutions, supervise the application of relevant techniques, take charge of international cooperation regarding the spam issue and provide anti-spam information to the public.

However, any transaction arising from emails will be charged to the Fair Trade Commission, the Consumer Protection Commission and other competent authorities, not the NCC.¹¹⁸

7.5 Contents of the Draft of Reg.

1. Objective of the Draft of Reg.: the NCC referred to the Can-Spam Act of 2003, the spam Act, directives on privacy and electronic

¹¹⁷ 參教育部網站：案例九濫發商業電子郵件，
http://www.edu.tw/EDU_WEB/EDU_MGT/MOEC/EDU0688001/tanet/tanet-IPR/94plan/06_02_09.htm 最後參觀日 2006/8/4

¹¹⁸ The relevant issues Q&A of draft governing commercial electronic email abuse act.

communications, Privacy and Electronic Communication Regulations 2003 to set Draft of Reg.. The objective of Draft of Reg. is to maintain the convenient use of the Internet, minimize harassment resulting from abusing commercial electronic mails and enhance the security and efficiency of the Internet environment.

2. Commercial Electronic Mail: this Draft of Reg. is only limited to any electronic mail transmitted by means of the Internet for the purpose of marketing products or commercial service.¹¹⁹ As we know, this Draft of Reg. regulates only “illegal transmission” and “commercial electronic mail”, excluding the information in electronic mails and other methods of transmission such as SMS, MMS, VOIP and so on. ¹²⁰Besides, in order to protect the freedom of speech, the subject of this Act is limited to commercial electronic mails, excluding other types of emails such as political speeches.
3. Opt-out mechanism: the NCC considers that it could be difficult for senders to receive prior consent from recipients, and prohibiting senders from using personal information will bring about substantial impact. Hence, it is practical to set up the opt-out mechanism, i.e., through the reply of recipient.
4. Self-regulation Requirement: the competent authority may require ISPs to establish national “Do not mail” data.¹²¹
5. Civil Damages: this Act sets only civil damages, including damages and non-pecuniary loss. Due to likelihood of inconvenient use/ time consumption and difficulty to prove damage, the compensation will range from NTD 500 to NTD 2,000 per email.¹²² A sender is liable

¹¹⁹ Article 2(1) of the Draft Reg.

¹²⁰ 行動簡訊具有下列性質，而未納入本法規範：(1)必須發送方與接受方的行動通訊業者有所協議，才可互通行動簡訊(2)依據電信法規要求行動簡訊的傳送，必須附帶發送來源的辨識碼，否則不得發送(3)目前行動簡訊引發問題，在於其所傳輸之內容與濫發垃圾郵件的規範，係針對其不當行為有所不同，因此，在管制模式上應有所不同(4)目前行動通訊業者透過訂型化契約的方式，約定使用者不得有「傳送不實資訊予不特定人」的義務，因此業者已透過自律方式，以軟體過濾不當簡訊的發送。

¹²¹ Article 6 of the Draft Reg.

¹²² Article 7 (3) of the Draft Reg. .

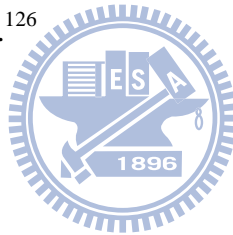
for damages by reason of the same cause and fact, not exceeding NTD 20 million.¹²³

6. Joint Liability: any advertiser or advertising agent who knew or should have known that commercial electronic mails conveyed by the commissioned sender in violation of Articles 4 and 5 of this Act, shall be jointly liable for any damages to the sender.¹²⁴

7. Class Action: a foundation may file a legal action in its own name with respect to the damages caused by the infringement of this Act, after having been so empowered by not less than 20 persons who have suffered loss or injury.¹²⁵

8. International Cooperation: the competent authority may cooperate with the relevant international organizations to exchange sources, methods of tracing, and other related information of commercial electronic mails.¹²⁶

Chapter 8 Conclusion



8.1 International

Though every country has established its respective regulations on spammers, spammers have been smart enough to flee into other countries which never set regulations on spam or only set lenient regulations to avoid being punished by judicial authorities. In order to solve this problem, the OECD conducted a survey and provided some solutions to the spam issues in developing countries. Recently, more and more International organizations have been established to fight spam.

The existing national organization can only serve as the interface for exchanging information and discussion of cooperation. There is no complete model to solve cross-boarder spam and practical methods are still under development. In addition, there is no balance between cost of surveying

¹²³ Id.

¹²⁴ Article 7(5) of the Draft Reg.

¹²⁵ Article 9 of the Draft Reg.

¹²⁶ Article 14 of the Draft Reg.

origin of spammers and punishment of spammers. Whether ISPs strictly enforce their regulation with users can affect the issues of spammers. More international efforts are needed to clear up spam.

8.2 Taiwan

In order to advance substantial public interest, our country has adopted some restrictive measures on regulation of speech. Following the frequency of e-commerce, our country has put more stress on spam, and referred to other countries' legalizations and drafts "Regulations Governing Abusing of Commercial Emails".

It is my opinion that the subject under these draft regulations is not as broad as those under regulations of the USA or EU. Our draft regulations are limited to email and do not include other subjects transmitting spam such as mobiles, Instant Messaging, SMS, MMS, VOIP, Bluetooth and so on; therefore, there will be a loophole in these regulations. The competent authority should consider expanding the subjects. In addition, the remedy under these draft regulations is the claim for civil damages against infringement. However, unlike the USA, which sets the injunction against spammers, infringers in this country may continue to transmit spam to users if he/she releases his/her property from liabilities. Finally, as in the USA and the EU, though the draft regulations may require correlative groups to set National Do Not Email Registry proposed by the competent authority, this information can also be used by those spammers if we can not trace the identification of spammers technically.

Reference:

Periodical (English):

1. Adam Mossiff, Spam-Oy, It's such a Nuisance (2004)
2. Cooley Alert, the Can-SPAM Act How it affects You, Cooley Godward LLP (2004).
3. Don Passenger and Jeff Kirkey, Information Technology Law: un-canned Spam: getting it back in the tin, 82 MI Bar Journal (March, 2003)
4. False Claims in Spam, a reported by the FTC's Division of Marketing Practices, April 30,2003.
5. Gray J. Fechter and Margarita Wallach, Spamming and other advertising issues: banner and pop-ups, ALI-ABA course of study materials, April 2005.
6. Fair Trade Commission, National Do Not Email Registry, a report to Congress, Federal Trade Commission, June 2004.
7. Nicola Lugaresi, European Union v. Spam: A Legal response, Trento University, Law School
8. Spam Issues in development countries, Directorate for science, technology and industry committee on consumer policy, committee for information, computer and communication policy, Organization for Economic Co-operation and Development(May 26, 2005)
9. Task Force on Spam, Anti-Spam Regulation, Directorate for science, technology and industry committee on consumer policy, committee for information, computer and communication policy, Organization for Economic Co-operation and Development (Nov. 15, 2005)
10. Nettleton Ewan, Legal update: getting though on Spam? The Journal of Database Marketing & Customer Strategy Management, Volume 12. Number 4 (2005)
11. MessageLabs Intelligence 2005 Annual Security Report.
12. Commission of the European Communities, Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 15.11.2006, COM (2006) 668 final.
13. Jorg Hladjk, Effective EU and US approaches to spam? Moves towards a co-ordinated technical and legal response-Part II, Communication Law, Vol.10 No.4 (2005)
14. Enrico Blanzieri and Anton Bryl, A Survey of Anti-spam Techniques,

Department of Information and Communication Technology,
University of Trento (2006)

15. Political Email: Protected Speech or Unwelcome Spam? Duke L. & Tech. Rev, 0001 (2003)_
16. Communication From the Commission to the European Parliament, the council, the European Economic and Social Committee and the committee of the Regions on Fighting spam, spyware and malicious software, COM (2006) 688, Brussels (2006).

Chinese:

1. 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. 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)。
3. 行政院經濟建設委員會，濫發電子郵件行為之管理與法制規範研究期末報告(2003)。
4. 林子儀，商業性言論與言論自由，美國月刊，二卷 8 期(1987)。
5. 李婉萍，防堵垃圾郵件立法審議中，RUN! PC (2005)。
6. 洪志郎，你有權拒絕 Spam 造訪你家，網路資訊(2006)。
7. 高銘鍾，病毒傳播篇-擊潰病毒與垃圾郵件的聯手攻擊(2005)。
8. 楊正瑀，返垃圾郵件，政府，網路使用者皆有責任，Source 週報 (2003)。
9. 我們應訂定返垃圾郵件法圖利 ISP 嗎?資安觀察(2005)
10. 黃立、蔡欣惠，從美國聯邦貿易委員會研究報告看「未經邀約的商業電子郵件」表示主旨欄之必要性，律師雜誌 311 期(2005)。
11. 黃菁謚，「濫發商業電子郵件管理條例」草案再檢視，律師雜誌 311 期(2005)。
12. 網路花絮:垃圾郵件一年花你 30 小時，政府機關資訊通報(2005)。
13. 劉邦典、林俊宇，垃圾郵件的氾濫宇危害分析，績效與策略研究 (2005)。
14. 簡維克、林雅惠，小心！垃圾電子訊息正侵入你的手機-以財產權及隱私權面向論立法規範垃圾簡訊之必要性，清華科技法律與政策論叢(2005)。
15. 賀祥宏，中華民國憲法，來勝出版，93 年 8 月。
16. 蔡甘子，亞洲垃圾郵件面面觀，網路通訊雜誌(2005)。
17. 蔡蕙芳，與垃圾郵件有關的刑法問題，律師雜誌 311 期(2005)。
18. 周慧蓮，行動簡訊國際規範趨勢，律師雜誌 311 期(2005)。

19. 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)。
20. 誠君，以白名單和過濾器防止垃圾郵件氾濫，Hope Net 科技月刊(2004)。
21. 戴君豪、黃菁濫，淹沒稻穗的雜草-談垃圾郵件法律管制策略，研考雙月刊(2005)。
22. 畢建同，挑戰 Anti-spam 的技術極限-現實與理想之間的距離，網路資訊雜誌(2004)。

Internet:

1. <http://www.cpc.gov.tw> The Consumer Protection Commission, Administrative Yuan.
2. <http://www.ftc.gov> Federal Trade Commission
3. <http://www.epic.org/reports/sufer-beware.html> Super Beware: personal privacy and the Internet, electronic privacy information center
4. <http://www.gigalaw.com> the impact of state anti-spam laws
5. <http://www.ftc.gov/os/2004/10/041012londonactionplan> The London Action Plans on International Spam Cooperation Enforcement Cooperation
6. http://www.edu.tw/DEU_WEB/EDU_MGT/MOECC?EDU0699001/tanent/tanet-IPR/94plan/06_02_09.htm940119 濫發商業電子郵件管理條例草案行政院第 2924 次院會通過版
7. <http://www.fcc.gov> Federal Communication Commission