هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

# Communication and Information Technology Commission

# BENCHMARKING OF SELECTED INTERNATIONAL BODIES AND INITIATIVES

**Final Version**

**19/09/2007**

Submitted to:

Submitted By:

# Acceptance of Deliverable

| | |
|---|---|
| Name | |
| Title | |
| Role | |
| Signature | |
| Date | |

# Document Control Page

| *Document Amendment Record* | | | |
|---|---|---|---|
| Change No. | Date | Prepared by | Brief Explanation |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## *Table of Contents*

# 1. PURPOSE OF THIS DOCUMENT

The purpose of this document is to review and analyze various anti-SPAM resources released by selected international bodies and initiatives. These resources include web sites, conferences, international agreements, volunteer activities, white papers, Request for Comments and others.

Relevant recommendations, practices and guidelines are extracted and highlighted in this document.

# 2. OUR APPROACH

Several international bodies have proposed a number of measures over the years to address SPAM. Recognizing that a single pronged approach to addressing SPAM would not be effective, these measures focus on various approaches to deal with SPAM.

## 2.1 IDENTIFICATION OF RELEVANT INTERNATIONAL BODIES AND INITIATIVES TO BE INCLUDED IN THE BENCHMARKING EXERCISE[1]

The approach used to identify these international bodies and initiatives was to review published information about a number of these bodies, with a focus on confirming their involvement in combating SPAM. While a number of the selected references are well-known international bodies, others represent Agreements or Cooperative initiatives entered into by two or more countries to fight SPAM.

A table showing the relevance of each international body/organization to the Spam-related areas is supplied at the end of the document.

### 2.1.1 THE INTERNATIONAL TELECOMMUNICATION UNIONS (ITU)

The International Telecommunication Union (ITU) is an international organization established to standardize and regulate international radio and telecommunications.

The ITU headquartered in Geneva, Switzerland is an international organization within the United Nations System where governments and the private sector coordinate global telecom networks and services. It is comprised of 191 state members from across the globe, and it has 3 sectors, namely the Radio communication sector, Standardization sector, and the Development sector.

The ITU promotes the exchange of information and best practices and provides support to developing countries in the field of spam.

Further, ITU has created an informal network of regulators and policy makers operating in the field of anti-spam activities, providing reliable information and data, and offering a platform to facilitate discussion and exchange of experiences. Moreover, ITU provides whitepapers, and documents related to Spam.

### 2.1.2 THE ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

The Organisation for Economic Co-operation and Development (OECD) is an international organisation of those developed countries that accept the principles of representative democracy and a free market economy.

The OECD groups 30 member countries sharing a commitment to democratic government and the market economy. With active relationships with some 70 other countries and economies, NGOs and civil society, it has a global reach. Best known for its publications and its statistics, its work covers economic and social issues from macroeconomics, to trade, education, development and science and innovation. It plays a prominent role in fostering good governance in the public service and in corporate activity, and helps governments to ensure the responsiveness of key economic areas with sectoral monitoring. By deciphering emerging issues and identifying

[1] For further information regarding the International Bodies and Initiatives, please refer to Appendix A.

policies that work, it helps policy-makers adopt strategic orientations. It is well known for its individual country surveys and reviews, internationally agreed instruments, decisions and recommendations to promote rules of the game in areas where multilateral agreement is necessary for individual countries to make progress in a globalised economy.

Among other activities, they offer a formal Anti-Spam website: “Task force in Spam” covering the following spam-related areas:

- Law & regulation;
- Enforcement;
- Technical solution;
- Education; and
- Statistic & data.

### 2.1.3 SPAMHAUS

The Spamhaus Project is an international non-profit organization whose mission is to track the Internet's Spam Gangs, to provide dependable real-time anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spammers worldwide, and to lobby governments for effective anti-spam legislation.

### 2.1.4 SEOUL-MELBOURNE ANTI-SPAM AGREEMENT[2]

Seoul-Melbourne Anti-Spam Agreement consists of twelve Asia-Pacific communications and Internet agencies that have joined the Australian Communications Authority (ACA) and the Korean Information Security Agency (KISA) in signing the Seoul-Melbourne Anti-Spam Agreement12, a multilateral memorandum of understanding (MoU) on cooperation in countering Spam. The MoU is focused on sharing knowledge, information and intelligence about known sources of spam, network vulnerabilities, methods of spam propagation, and technical, education and policy solutions to the spam problem.

### 2.1.5 WORKING GROUP ON INTERNET GOVERNANCE (WGIG)

The Working Group on Internet Governance (WGIG) is a United Nations multi stakeholder working group set up after the 2003 World Summit on the Information Society (WSIS) first phases Summit in Geneva to agree on the future of Internet governance.

The main activity of the WGIG is to investigate and make proposals for action, as appropriate, on the governance of Internet.

WGIG established public policy areas for the issues relating to the use of the Internet, including Spam, network security and cybercrime. While these issues are directly related to Internet governance, the nature of global cooperation required is not well defined. It is important to note that OECD works on WGIG-designated public policy issues because many of the priority issues for the WGIG are also priority areas for the OECD, specifically the OECD Committee for Information, Computer and Communications Policy (ICCP)."

[2] A copy of Seoul-Melbourne agreement can be found at: http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam-multilateral_mou-seoul-melbourne_agreement-draft.pdf

### 2.1.6 Asia-Pacific Economic Cooperation Telecommunications & Information Working Group (APEC)

APEC TEL WG is the Asia-Pacific Economic Cooperation Telecommunications & Information Working Group. The Telecommunications & Information Working Group (TEL WG) is committed to improving the telecommunications and information infrastructure in the region and to facilitating effective cooperation, free trade and investment and sustainable development. The TEL's program of action covers different activities including:

- E-security;
- E-government; and
- Hosting meetings and conferences regarding Spam.

### 2.1.7 The Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE)

APCAUCE is the Asia Pacific wing of CAUCE, the Coalition Against Unsolicited Commercial Email. CAUCE is the world's largest volunteer anti-Spam organization, with chapters in the USA, Canada, the EU and over a dozen economies in the Asia Pacific region.

### 2.1.8 The Anti-Phishing Working Group (APWG)

The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing and the spread of crimeware that automatically mines consumers' personal data from their PCs. Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. There are currently over 1500 organizations participating in the APWG and more than 2400 members worldwide..

Further, the organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks. APWG provides a Report-Phishing service by building a repository of phishing scam emails and websites to help people identify and avoid being scammed in the future. Moreover, they provide technical whitepapers and briefings from APWG Sponsors, such as : McAfee, Symantec and RSA Security.

### 2.1.9 Messaging Anti-Abuse Working Group (MAAWG)

Messaging Anti-Abuse Working Group (MAAWG) is a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. MAAWG is where the messaging industry comes together to work against SPAM, viruses, denial-of-service attacks and other online exploitation. MAAWG addresses messaging abuse by systematically engaging all aspects of the problem, including technology, industry collaboration and public policy.

The MAAWG is a group of telecommunications companies brought together by OpenWave[3] in early 2004. The purpose of the group is to fight spam, phishing, and other possible forms of e-mail abuse. MAAWG Spam-related activities & services include:

[3] A commercial provider of software solutions for the communications and media industries.

- Getting the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging spam;
- Running Anti-Spam workshops; and
- MAAWG worked together with the OECD Anti-Spam Task Force & developed an E-mail Metrics Program and agreed on a series of ISPs spam indicators to measure:
    - ➢ The total number of dropped connections resulting from IP blocking (while this parameter may be imprecise, it gives a sense of the magnitude of the amount of messages which are not penetrating the networks).
    - ➢ The total number of blocked or tagged inbound e-mails and percentage of e-mails going through the ISPs (excluding blocked connections) that are identified as spam.
    - ➢ The focus is therefore on "unwanted" e-mail, so that the difficulty of defining spam will be avoided.

### 2.1.10 The Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standard bodies.

The IETF is formally an activity under the umbrella of the Internet Society. Request for Comments (RFCs) are a series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies.

Two RFCs are relevant to "Spam": RFC 2635 and RFC 2505.

- Request for Comments: 2635 "A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)", June 1999; and
- Request for Comments: 2505 "Anti-Spam Recommendations for SMTP MTAs", February 1999.

### 2.1.11 London Action Plan (LAP)

An international action plan designed to encourage communication and cooperation between countries in tackling spam and spam-related problems. Membership includes broad range of spam enforcement agencies, including data protection agencies, telecommunications agencies and consumer protection agencies.

The purpose of this Action Plan is to promote international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses.

### 2.1.12 GSM Association

The GSM Association (GSMA) is a global trade association representing over 700 GSM mobile phone operators across 218 countries of the world, and more than 200 manufacturers and suppliers support the Association's initiatives as associate members.

### 2.1.13 MOBILE MARKETING ASSOCIATION

The Mobile Marketing Association (MMA) is the premier global association that strives to stimulate the growth of mobile marketing and its associated technologies. The MMA is a global organization with representation in over twenty countries.

### 2.1.14 REGIONAL ENTITIES/BODIES

The following regional entities and bodies will be considered **as applicable**:

- **The Arab League:** The Arab league is an association of Arab states established in 1945 to promote cooperation among member nations in matters relating to economic and social development and foreign policy. Numerous specialized organizations and other institutions that promote Arab cooperation and protect Arab interests in a wide array of fields fall under the league umbrella. One of the specialized organizations in this association is the Arab Telecommunications Union.
- **The Gulf Cooperation Council (GCC):** The GCC seeks to promote coordination between member states in the Arab Gulf in all fields in order to achieve unity.
- **The Arab ICT Regulators' Network:** The Arab ICT Regulators' Network is an independent organization created at the ITU's first Arab Regulators meeting in Algiers in April 2003, with the objective of sharing experiences and developing expertise that will enable Arab ICT regulators to facilitate growth in telecom products and services and achieve equality of access to such services and products in the Arab region.

### 2.1.15 MESSAGING PROVIDERS

Messaging providers provide email services accessible from a Web browser anywhere in the world. They offer free accounts worldwide with features such as spam filters and enhanced virus scanning. Moreover, they offer Spam reporting service, Spam monitoring and statistics.

The following messaging providers will be considered as applicable:

- Yahoo;
- Hotmail; and
- Gmail.

## 2.2 DEFINITION OF A STRUCTURE TO FACILITATE THE BENCHMARKING EXERCISE

In order to review these measures in a systematic and structured manner, the anti-SPAM component framework recommended by OECD was used to structure our analysis. Since the OECD framework was considered comprehensive a number of countries appears to have used the OECD framework, it was decide to use this framework for our benchmarking study.

The OECD Task Force, charged with developing a framework aimed at tackling SPAM using a broad multi-disciplinary range of solutions, recommended a range of policies and measures for inclusion within a comprehensive public anti-SPAM policy framework.

The Anti-SPAM measures recommended by OECD were structured into policy components focused on:

- Regulatory approaches;
- Enforcement co-operation;
- Industry driven activities;
- Technical solutions;
- Education and awareness initiatives;
- SPAM measurement[4], and
- International co-operation and exchange.

In structuring the policy framework into these components, OECD made specific recommendations with regard to each, that are also useful to consider while developing the anti-SPAM policy framework in Saudi Arabia.

## 2.3 INTERNATIONAL BODIES: FIELDS OF INTEREST

The table below summarises the applicable components to be addressed for each international body and organization.

| | **Regulatory Approaches** | **Enforcement Co-operation** | **Industry Driven Activities** | **Technical Solutions** | **Education and Awareness** | **SPAM Measurement** | **International Co-operation & Exchange** |
|---|---|---|---|---|---|---|---|
| **ITU** | X | X | X | X | X | | X |
| **OECD** | X | X | X | X | X | X | X |
| **SPAM-HAUS** | | | | X | X | | |
| **LAP** | | X | | | | | X |
| **WGIG** | | | | | | | X |
| **APEC** | | | | | | | X |
| **APCAUCE** | | | | | X | | X |
| **APWG** | | | | X | | | X |
| **MAAWG** | | | X | X | | X | X |
| **GSMA** | | | X | | X | | |
| **MMA** | | | X | | X | | |
| **IETF** | | | | X | | | |
| **Messaging Service** | | | | | X | | |

[4] The terms 'SPAM Measurement' and 'SPAM Metrics' are used interchangeably by OECD, but they refer to one thing: monitoring the impact of anti-spam measures to assess their effectiveness.

| | Regulatory Approaches | Enforcement Co-operation | Industry Driven Activities | Technical Solutions | Education and Awareness | SPAM Measurement | International Co-operation & Exchange |
|---|---|---|---|---|---|---|---|
| Providers | | | | | | | |
| Seoul-Melbourne Agreement | | | | | | | X |

### 2.3.1 Regulatory Approaches

The development of an anti-SPAM legislation that tackles SPAM and related problems is fundamental. The anti-SPAM regulation should attempt to:

- Preserve the benefits of electronic communications;
- Prohibit and take action against the act of SPAMming; and
- Reduce the amount of SPAM.

The regulatory approach will be reviewed, where applicable, based on the following eleven elements as per OECD guidelines[5]:

- Technical Elements
- Consent
- Privacy
- Commercial Elements
- Bulk
- In breach of fair trade
- Criminal or pornographic Content
- Damage
- Requirements for Legitimate Messaging
- Exemptions or Restrictions
- Address harvesting and Dictionary attacks

### 2.3.2 Enforcement

While having the appropriate legislation is indeed necessary, implementation and application of the law is fundamental. Particular attention in the context of SPAM should be given to national co-ordination, sanctions, empowerment of enforcement authorities, and cross-border enforcement co-operation.

### 2.3.3 Industry Driven Initiatives

In order to appropriately deal with SPAM, generally-applicable anti-SPAM laws should be coupled with self-regulatory initiatives undertaken by private sector players, such as Internet

[5] These elements are considered comprehensive in terms of their coverage to the regulatory approach. Most countries have implemented all or most of those elements. Needless to say, those components should be customised according to the domestic legal system while taking into consideration the environmental and cultural aspects.

Service Providers, e-mail service providers, telecommunication operators, direct marketers, online operators, software companies, and their others.

### 2.3.4 TECHNICAL SOLUTIONS

Anti-SPAM tools operate at many levels – at the point of origination of e-mail, in the backbone network, at the gateway and on the recipient computer – and may be used alone or in combination. Any attempt to combat SPAM effectively must involve the sensible application and administration of a number of these technological tools and methods as well as factors to consider prior to their implementation. No method will be entirely successful in isolation. When a number of anti-SPAM technologies are effectively used in collaboration with one another, the effect can be to drastically reduce the level of SPAM impacting a system.

### 2.3.5 EDUCATION AND AWARENESS

A comprehensive anti-SPAM strategy must ensure that the end-user, who is the final recipient of SPAM, the possible victim of viruses and scams, and, at the same time, the person who has control over their computer and personal information, is sufficiently educated and aware of how to deal with SPAM and other online threats. Education and awareness raising activities are needed in large enterprises, small and medium enterprises, for residential users and in education establishments. They must aim to create a culture of security, and encourage a responsible use of cyberspace.

### 2.3.6 SPAM MEASUREMENT

Measurement is critical to evaluating the evolution of SPAM and the effectiveness of anti-SPAM solutions and educational efforts, to be able to determine if a strategy is effective, and eventually what changes are needed in policy, regulatory and technical frameworks.

Governments and private sector players should monitor the impact of anti-SPAM measures, to assess their effectiveness. ISPs, other network operators, and national anti-SPAM agencies should, to the extent possible, share information and data on the intensity and scope of SPAM and its evolution. Measuring methods should be detailed and documented, in order to improve the legibility of the results obtained.

### 2.3.7 INTERNATIONAL CO-OPERATION AND EXCHANGE

Global co-operation is fundamental to promote appropriate domestic frameworks to counter SPAM in all countries, and to encourage co-operation among governments, private sector, civil society and other stakeholders, in order to ensure the harmonized and widespread application of technical measures and the effective enforcement of applicable rules.

Why using these components?

The use of these components to structure the benchmarking review has a number of benefits including:

- Adequate focus on key components
- Completeness of the review
- Use as a reference while developing individual components of the Anti-SPAM policy framework for Saudi Arabia

Accordingly, this report describes each component as it is addressed by the relevant international body or organization.

# 3. EXECUTIVE SUMMARY

SPAM represents a major annoyance and threat to ICT applications users and is spreading into all means of communications like mobile phones, facsimile transmissions, and SPAMmers are always on high-alert to exploit any new technology in order for them to achieve their goals.

Many countries, regional and international organizations, bodies, and working groups have taken steps to deal with the issue of SPAM. Anti-SPAM policy frameworks have been used in a number of countries to combat SPAM and many other countries are considering developing such frameworks.

As Saudi Arabia is willing to develop an anti-SPAM framework, and besides benchmarking against other countries, it was necessary to identify the well-known international bodies involved in the fight against SPAM, reviewing and analyzing their outstanding practices and guidelines, and ultimately adapting and using this information as a base to help in developing the anti-SPAM framework in the Kingdom of Saudi Arabia. Examples of those international bodies are: the Organization for Economic Co-operation and Development (OECD), the International Telecommunication Union (ITU), the Anti-Phishing Working Group (APWG), the Messaging Anti-Abuse Working Group (MAAWG) and others.

The review was structured according to OECD recommendations. Thus, this document reviews, examines and extracts the best practices developed by the various international bodies in the following areas:

- Regulatory approach;
- Enforcement cooperation;
- Industry driven initiatives;
- Technical solutions;
- Education and awareness initiatives;
- SPAM measurement; and
- International Cooperation and Exchange.

Leading practices and recommendations released by those international bodies, where applicable, have been summarized below.

***Regulatory***

The development of anti-SPAM legislation that tackles SPAM is fundamental. Legislation sets clear directions on what is allowed and what is not allowed. Since SPAM horizontally spans multiple areas, it touches upon telecommunication services, consumer protection, security, and privacy, at national and cross-border levels.

The anti-SPAM regulatory framework has multiple sub-components and according to OECD, it is recommended that the anti-SPAM regulatory framework is broken down into elements which should be considered as far as possible, taking into account each country's institutional and legal framework. These elements are: Technical elements, consent, privacy, commercial elements, bulk, content (fair trade, criminal or pornographic content), damage, requirements for legitimate messaging, exemptions or restrictions, and address harvesting and dictionary attacks. Even with these almost agreed-on elements in place, typically we find zones of divergence in legal approaches to spam. These differences often derive from diverging views on what constitutes permissible communication or the most efficient way to achieve enforcement. Examples of points of divergence are: the consent requirements: shall the consent be obtained prior to sending a message? Is one message considered as SPAM? Or only if sent in bulk? enforcement, that is, who is permitted to recover for or prosecute violations of the law and, in particular, whether private entities such as ISPs and SPAM recipients may recover damages?

Unfortunately, there is no common definition for SPAM and according to ITU and OECD, there are widespread typical features distinguishing a SPAM message, namely: an electronic message, with false or hidden origins, having non valid unsubscribe option, carrying illegal or offensive content, utilising of addresses without the owner's consent, and sent in bulk or repetitively.

What outcomes should be achieved by the anti-SPAM legislation? And what are the characteristics of a successful anti-SPAM legislation?

According to OECD, an anti-SPAM legislation should preserve the benefits of electronic communication, prohibit and take action against SPAMmers, and reduce the amount of SPAM. Moreover, it should conform to four general principles: Simplicity, effective enforcement, having appropriate international linkages, and providing a clear policy direction where the main objectives of the national and international anti-SPAM policy are outlined at an earlier stage and need to underline the entire governmental strategy.

In conjunction with OECD recommendations, ITU advises that anti-SPAM law should:

- Focus on content with commercial nature;
- Ban fraudulent or misleading messages;
- Prohibit concealing of falsifying a message's sender, advertiser, or routing information;
- Draft regulations covering Internet communication generally rather than specifying applications such as email;
- Require senders to provide recipients with unsubscribe facility, respect the recipient's requests, and prevent senders from exchanging or selling addresses or recipients who unsubscribe;
- Prohibit address harvesting and dictionary attacks, along with software tools specifically tailored to these purposes; and
- Seek to standardise labelling requirements.

***Enforcement***

According to OECD, enforcement is a fundamental issue, which, if not dealt with appropriately, can make a good piece of legislation useless. For this reason, it is recommended by OECD to put in place an effective sanction regime and appropriate standards of proof. In addition, appropriate powers and resources need to be allocated for enforcement authorities.

ITU and OECD recommend that countries should establish SPAM enforcement authorities. Mainly, one agency should be assigned as the nodal enforcement agency and serves as a coordinator at the national level among other national enforcement agencies (if existing) and as a contact point for foreign authorities to facilitate cross border co-operation. SPAM enforcement authorities should have the necessary authority and investigative power to obtain evidence sufficient to investigate and take action in a timely manner against violations of laws targeting the senders of SPAM and the individuals or companies that profit from the sending of such communications. Cooperation with relevant private sector is essential as well.

As a proactive approach, countries should review periodically their own domestic frameworks and take steps to ensure their effectiveness for cross-border co-operation in the enforcement of applicable laws. In fact, co-operation at the national level would be particularly important to avoid duplication of activities, and allow the optimization of resources and the exploitation of synergies between the different players. In this regard, national legislation could facilitate information sharing and mutual assistance between competent authorities in different countries through bilateral and/or multilateral agreements and by participating in international bodies and enforcement cooperation initiatives such as London Action Plan (LAP), OECD and ITU.

***Industry driven initiatives***

Industry driven initiatives, or self regulatory activities, are activities initiated by the industry, either being imposed by the local enforcement authorities, or when there is a need for the industry to take some action against SPAMming activities. Private sector players such as ISPs, telecommunications operators, and direct marketers, play a critical role in the fight against SPAM. In fact, all the countries involved in the battle against SPAM have coupled their anti-SPAM laws with self-regulatory initiatives mainly through the development of codes of conduct for ISPs and e-marketers and making these codes either binding or voluntary. Other form of industry assistance is reflected in awareness programs, software products, sharing information, etc. In this context, OECD and ITU urge industries, including service providers, direct marketers, and software makers to adopt best practices in order to combat SPAM. In particular, Governments and regulators should support the development of codes of practice for electronic marketing and ISPs. Moreover, improved cooperation on enforcement between industry and enforcement authorities should also be promoted.

For instance, in the USA, ISPs include anti-SPAM clauses in their Acceptable Use Policy (AUP). Another example is the GSM Association (GSMA) and the Mobile Marketing Association (MMA) which developed a Mobile SPAM Code of Practice where mobile operators commit to include anti-spam conditions with all new contracts and provide a mechanism to ensure appropriate customer consent and control with respect to mobile operators' own marketing communications.

***Technical solutions***

Although legislation, government action and industry assistance are fundamental, solutions to eliminating SPAM need to be supported by appropriate technical measures. Anti-SPAM tools that operate at different levels together, with the proper administration and monitoring, make up the technical solutions to SPAM.

In this regard, OECD believes that judicious application of technology should be the backbone of any approach that aims to defeat SPAM. Indeed, none of the technologies acts as a "silver bullet" or one-stop solution to the problems created by SPAM; instead, all of the technologies are complementary and will be most effective when implemented in conjunction with each other.

It is recommended that Internet Service Providers and other network operators should constantly improve their knowledge and operating practices, and update their technical best practices in order to face new challenges and technological evolution and promote the implementation and sharing of available technical solutions among providers.

There are different anti-Spam technologies that are used to fight Spam. Typically, anti-SPAM technologies can be based on filters, authentication, and blacklists/white lists which might be augmented to filters. These technologies can be deployed at the client side or the gateway. According to ITU and OECD, each of the available technologies has its weaknesses and strengths and the integration of a number of technologies is crucial to reduce the impact of SPAM.

***Education and awareness***

Increasing education and awareness is a crucial part of a comprehensive anti-SPAM strategy. Simply, one of the reasons why SPAMmers are successful is that some e-mail recipients are still responding to SPAM and purchasing advertised products or services, visiting websites advertised by SPAMmers, or being tricked into responding to requests for personal information from 'phishing' scams.

SPAM awareness programs might be sponsored by different entities such as SPAM law enforcement agencies, governmental and non-governmental organizations. They should target different stakeholders such as end users, ISPs and e-marketers. Moreover, it might take different forms such as creating Web sites, hosting SPAM-related conferences, releasing guidelines and best practices, and others.

According to OECD, SPAM awareness and education should target students, children, individuals, Internet Service Providers (ISPs) and Email Service Providers (ESPs), business entities, especially small and medium enterprises (SMEs) and recommends that governments, direct marketers, user's groups, large companies and SMEs, and industry corporations should launch awareness programs.

Governments, as per ITU recommendations, should make sure that consumers are aware of where they can complain, what will be investigated, what action may be taken, and what information they need for authorities to launch an investigation.

***<u>SPAM Measurement</u>***

SPAM measurements are the ways used to report the effectiveness of the SPAM solutions being deployed to combat SPAM. Measurement is very critical to evaluating the evolution of SPAM and the efficacy of anti-SPAM solutions and educational efforts, to be able to determine if a strategy is effective, and eventually what changes are needed in policy, regulatory and technical frameworks.

In this regard, OECD mentions that:

- Governments and private sector players should monitor the impact of anti-SPAM measures, to assess their effectiveness.
- ISPs, other network operators, and national anti-SPAM agencies should, to the extent possible, share information and data on the intensity and scope of SPAM and its evolution.
- Measuring methods should be detailed and documented, in order to improve the legibility of the results obtained.

Ideally, government and private sector monitor the impact of anti-SPAM measures. Several firms provide mechanisms to collect statistics which is used ultimately to describe SPAM such as the Messaging Anti-Abuse Working Group (MAAWG) email metrics program which is used by the authorities in different countries.

***<u>International Cooperation and Exchange</u>***

Global co-operation is fundamental to promote appropriate domestic frameworks to counter SPAM in all countries, and to encourage co-operation among governments, private sector, civil society and other stakeholders, in order to ensure the harmonized and widespread application of technical measures and the effective enforcement of applicable rules. Countries involved in the battle against SPAM consider International cooperation as one of the pillars of the anti-SPAM framework. It contributes significantly in the fields of laws and regulations, enforcement, education and awareness and industry cooperation.

The international cooperation takes different forms through cooperating with regional and international entities, signing agreements, entering into MoUs, belonging to international bodies fighting against SPAM, sharing knowledge and raising awareness, and developing international industry codes and guidelines. In fact, and due to its importance of the global cooperation in the battle against SPAM, OECD recommends that:

- National co-ordination should be first priority;
- Cross-border enforcement against SPAM requires a global strategy to reach effectiveness;
- There has to be strategy in place that handles and organizes SPAM matters from around the world;
- Global outreach should be the objective;
- Action must be taken against SPAMmers no matter where they are, and hence, a reach out to the broadest possible coalition of enforcement agencies worldwide is needed;
- Adequate mechanisms for information gathering and sharing are needed for enforcement agencies to be able to investigate, preserve and obtain information and evidence and share that information with foreign counterparts in appropriate circumstances; and
- While informal frameworks (bilateral MoUs, multilateral or model MoUs, networks such as the London Action Plan) do indeed improve communication and working-level collaboration, a formal framework may be more appropriate to create a common stable and effective mechanism at global level.

Other international bodies have participated in the international cooperation by making proposals for action, as appropriate, on the governance of Internet as with the Working Group on Internet Governance (WGIG) or by developing set of characteristics to be considered in a code of conduct as an international initiative for all messaging providers as with the Messaging anti-abuse working group (MAAWG).

The problem of spam is complex, and a multi-stakeholder and multi-pronged strategy is fundamental. Developing an anti-SPAM framework is a multi-faceted battle that spans law, enforcement, industry assistance, technology, education and awareness, SPAM measurement, and international cooperation.

The anti-SPAM framework must take into consideration the legal, cultural and environmental aspects, be reviewed periodically, and should seek harmonisation with the international trends in the world to avoid cross-border problems and conflicts with other frameworks adopted in other regimes

# 4. SPAM COMPONENTS AS ADDRESSED IN THE SELECTED INTERNATIONAL BODIES AND INITIATIVES

This section is focused on reviewing the recommendations and guidelines provided by the selected international bodies and initiatives, using the policy framework components as the basis for the review.

## 4.1 REGULATORY APPROACH

### 4.1.1 OECD[6]

According to OECD, while different countries define SPAM in a manner that is most relevant to their local environment; there are common characteristics that countries have recognized in their SPAM definitions:

- Electronic message: SPAM messages are sent electronically. While e-mail is by far the most significant channel for SPAM, other delivery channels are also considered in a number of countries (mobile SPAM, such as SMS and MMS, SPAM over IP, etc).
- Hidden or false message origins: SPAM messages are often sent in a manner that disguises the originator by using false header information. SPAMmers frequently use unauthorized third-party e-mail servers.
- SPAM does not offer a valid and functional address to which recipients may send messages opting out of receiving further unsolicited messages.
- Illegal or offensive content: SPAM is frequently a vehicle for fraudulent or deceptive content, viruses, etc. Other SPAM includes adult or offensive content, which may be illegal in some countries, especially if it is sent to minors.
- Utilization of addresses without the owner's consent: SPAMmers often use e-mail addresses that have been collected without the owner's explicit consent. This is frequently done through software programmers which gather addresses from the Web or create e-mail addresses (harvesting and dictionary attacks).
- Bulk and repetitive: SPAM messages are typically sent in bulk in an indiscriminate manner, without any knowledge about the recipient other than the e-mail address.

#### Technical Elements

OECD advises that legislative definitions of SPAM focus on:

- ■ A particular messaging medium [E-mail, Instant Messaging, Short Message Service (SMS), etc.]; or
- ■ Attempt to provide a technology-neutral approach that provides an overarching statement of principles that is more broadly applicable. In this approach, it is worthwhile to evaluate which particular messaging media are being misused or causing problems within the jurisdiction, which media have a strong potential to

[6] *Source: The Organization for Economic Co-operation and Development (OECD). On (www.oecd-antiSPAM.org).*

be misused in the future, and which are unlikely to be misused within the jurisdiction.

## Consent

OECD describes[7] the pros and cons of the different types of consent as follows:

| Consent[8] | Pros | Cons |
|---|---|---|
| Opt-in (Express consent) | -Protect users' privacy, providing more control on personal data.<br>-It can result in a much higher response rate for legitimate online marketers as the messages are from known or trusted senders, and therefore are much more likely to be read and relevant to the recipient.<br>-The burden of proving that consent has been given lies with the sender of the message, not with the recipient. | -Difficulty in keeping records of received consent by business. The absence of such records may significantly restrict the potential pool of recipients who can be targeted for otherwise legitimate messaging.<br>-Restricts commercial free speech.<br>-Could result in devoting enforcement resources in areas where consumers are not financially[9] harmed. |
| Inferred and implicit consent | More flexible. | It may be difficult to define when a message can be related to an existing business relationship. |

[7] This table is taken from OECD resources ''as is''. Further analysis will be done in separate reports where appropriate.

[8] Expressed: Form of consent where an individual or organisation has actively given their permission to a particular action or activity (opt-in).

Inferred/implicit: consent which generally can be inferred from the conduct and/or other business relationships of the recipient.

Assumed consent: there is a presumption of consent until it is removed by the recipient, for example by .unsubscribing. (Opt-out).

[9] Assuming that SPAM is commercial in nature.

| Consent[8] | Pros | Cons |
|---|---|---|
| Assumed consent | -Less constrictive to the operation of online commerce; minimal risk of inadvertently proscribing legitimate messaging.<br>-Does not restrict choice of email recipients who want to receive commercial messages. | -It transfers the burden of effort and cost to the consumer.<br>-In order to unsubscribe the email must be opened and responded to, which is contrary to good e-security practice, unless the e-mail is from a known and trusted source.<br>-Unsubscribe links are often non-functional.<br>-It places the evidentiary burden upon the recipient of the message. |
| Blended approaches to consent | - | - |

## Commercial Elements

OECD states that, the majority of SPAM is sent in order to achieve a profit[10] – through the sale of goods of services, or through some sort of fraud. Arguably, one of the better ways of reducing SPAM is to reduce the economic benefits that the SPAMmer receives from sending SPAM messages. For this reason, many legislative definitions of SPAM stress the commercial nature of SPAM – that SPAM is sent for marketing purposes or to achieve financial gain. If there are concerns that regulatory efforts against SPAM could have negative impacts on freedom of speech[11] or expression, then a focus on commercial messages would clarify that personal, political, religious or ideological messages would not be restricted by anti-SPAM activities.

## Bulk

According to OECD:

- Bulk e-mail (Usually over 50-100 over 24 hours).
- One of the most significant problems with the bulk approach is its arbitrary nature; not all bulk e-mail is SPAM.

[10] Obviously, there are other kinds of SPAM messages having different nature that shall be considered as well.

[11] The scope of the right to free speech is subject to each country's restrictions and exemptions. The meaning of 'Freedom of Speech'' is customised according to the national, cultural, political, and religious values and interests.

## Damage

Legislative approaches to quantifying damages, particularly where a damage amount operates as a threshold to initiating a civil or criminal enforcement action, could include:

1. Assigning a set monetary damage amount to each piece of SPAM sent or received (e.g., Euro 1, GBP 1 or USD 1),
2. Measuring damage based on the number of affected recipients (e.g., an enforcement action could be initiated when at least 50 users within a jurisdiction are affected), or
3. Measuring damage based on the number of SPAM messages received by a single entity, without a requirement to demonstrate an actual monetary damage amount (e.g., an enforcement action could be initiated when a single user received more than 50 SPAM messages from the same entity within a defined time period).

## Requirements for Legitimate Messaging

The recipient of electronic messages should always be able to unsubscribe from the mailing list, requesting that such communication cease.

- Almost all legislation currently implemented foresees that a valid return address (or number) should be included in messages, so that the recipient may easily unsubscribe, without any additional cost. In some cases a postal address should also be provided.[12]
- The sender is given a period of time (for example 10 days) to comply and cease the transmission.
- Any transmission of messages after the recipient opted-out is not permitted.

OECD mentioned that:

- Labelling of e-mails as SPAM can be a useful tool in the fight against SPAM. (It has get weaknesses as well as depicted in the table below).
- Labelling is the use of standard words in the message header or subject line that clearly identifies the content of the message, for example, the use of "ADV" for advertising and "ADLT" for adult content.
- OECD outlines the advantages and disadvantages of 'labelling' as follows:

| Advantages | Disadvantages |
|---|---|
| Recipients are able to distinguish between advertising material and other e-mail traffic. | Variations on labelling may result in the evasion of filtering systems, for example, "A.D.V." or "a d v" instead of "ADV". |

[12] This is to ensure that the sender is known and the receiver can always contact the sender to opt out. According to the USA CAN SPAM Act, it is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message, among other requirements, provides 'a valid physical postal address of the sender.'

| Advantages | Disadvantages |
|---|---|
| Enable the more efficient and effective use of filtering systems. | Labelling would mostly be an effective anti-SPAM tool only if an internationally harmonized approach were adopted. This would be necessary to prevent problems emerging in relation to linguistic or alphabet differences between countries. |
| | SPAM offenders, especially those that obscure their identity and do not provide accurate contact details, are unlikely to comply with such a requirement. |

### Exemptions or Restrictions

According to OECD, the extent to which certain types of electronic messaging may be exempted from anti-SPAM regulation will depend on how SPAM is defined for the primary purpose of the regulation. For example:

- If SPAM is defined as “commercial” messaging, then exemptions may be appropriate for messages which have a commercial element but which are primarily non-commercial and which a government believes should not be prohibited.
- If SPAM is defined as “bulk” messaging, then exemptions may be appropriate for large-scale messaging which a government believes is in the public interest.

Possible exemptions:

- Government Bodies: Messaging from government bodies may be appropriate to enable dissemination of information in the public interest.
- Charities: Legitimate charities may reasonably wish to use electronic messaging for fund-raising and other purposes.
- Political Parties: Messaging from political parties may be seen as a legitimate expression of free speech.

### Address harvesting and Dictionary attacks

OECD states that, legislation may include specific provisions to levy additional sanctions if harvesting software and harvested address lists Dictionary attacks are used to aid the sending of SPAM in contravention of the jurisdiction’s SPAM legislation: the act of selling, acquiring or using harvesting software or harvested address lists, or the automatic generation of recipients. Addresses may be sanctioned.

### Criminal or pornographic Content

According to OECD, legislation may be drafted to particularly target criminal or pornographic messages, whether by making it part of the jurisdiction’s definition of SPAM, associating additional penalties to messages containing these elements, or, in the case of pornography, requiring additional measures of compliance (such as labelling).

## In breach of fair trade

OECD advises that, SPAM legislation may be drafted to require that goods and services advertised and/or offered in messages must be legal, accurately described and commercially responsible. This may be useful in jurisdictions where the coverage of existing domestic consumer protection laws and laws relating to misleading and fraudulent conduct in respect of online or electronic messages is not clearly drawn out. A focus on whether the content of a message is misleading or fraudulent leaves aside many of the systemic concerns of SPAM.

## Privacy

According to OECD, the regulation of SPAM may entail a significant overlap with privacy legislation and policies, and builds upon the idea that the use of personal data should be subject to acceptable (frequently legislatively determined) norms. Thus, the sender of messages may be required to comply with such requirements. However, it is worth noting that where such protection is available, it is only available to natural persons and not legal persons as privacy rights generally only attach to the former.

Data Protection regimes aim to regulate the use and abuse of personal data. To the extent that e-mail addresses are personal data, then use, exchange or selling of these may be seen as illegitimate invasions on the privacy of the addressee.

## OECD General SPAM - Related Legal Recommendations

National anti-SPAM regulation should attempt to:

- Preserve the benefits of electronic communications by increasing user trust in the Internet and electronic messaging media and improve the availability, reliability and efficiency of services, as well as the performance of global communication networks.
- Prohibit and take action against the act of SPAMming, as defined by national law. Legislation alone may not stop potential SPAMmers from taking advantage of this marketing technique, however laws and regulations can have an impact by sanctioning against those individuals and organizations that choose to make use of SPAM and profit from it. The value of legislation will depend on sanctions, in particular in the certainty of their application.
- Reduce the amount of SPAM. To prevent SPAM from being sent, activities need to be targeted at different stages, in order to reduce the volume of SPAM traversing networks, and reduce the number of SPAM received by end-users.

To achieve these goals, legislation should conform to four general principles:

- Policy direction: The legislation should provide a clear policy direction. The main lines and objectives of national and international anti-SPAM policy should be outlined at an earlier stage and need to underlie the entire governmental strategy.
- Regulatory simplicity: The legislation should be short and simple.
- Enforcement effectiveness: Enforcement is a fundamental issue, which, if not dealt with appropriately, can make a good piece of legislation useless. For this reason it is important to put in place an effective sanction regime and appropriate standards of proof. In addition, appropriate powers and resources need to be allocated for enforcement authorities.

- International linkages: As SPAM is a cross-border issue, legislation should foresee appropriate international linkages, and provide national authorities with the possibility to co-operate in investigations and exchange information with foreign authorities.

The role of Internet Service Providers and e-mail service providers is also important, and could be considered in legislation. In particular: governments and regulators should support the development of ISP codes of practice that complement and are consistent with legislation. Governments should encourage industry associations to develop such codes and adopt best practices where they are in the public interest and do not impose undue financial and administrative burdens on participants.

Legislation could also provide a comprehensxive framework to support the activities of ISPs to block or limit the circulation of SPAM e-mail. ISPs should be able to take appropriate and balanced defensive measures to protect their networks, and should be allowed to take legal action against SPAMmers[13]. Similar results could be achieved through appropriate contractual provisions between ISPs and users.

### 4.1.2 ITU[14]

The information of this section has been gathered based on ITU analysis of existing SPAM laws.

According to ITU analysis, a precise definition of SPAM does not exist but there is a fairly widespread agreement that SPAM exhibits the following general characteristics:

- SPAM is an electronic message. (For most purposes, this may be restricted to e-mail, but other methods of delivering SPAM do exist, including the Short Messaging Service, or SMS, etc.).
- SPAM is unsolicited[15]. If the recipient has agreed to accept a message, it is not SPAM. However, how and when such consent is given may not be clear, especially when a pre-existing relationship exists between the sender and recipient.
- SPAM is sent in bulk. This implies that the sender distributes a large number of essentially identical messages and that recipients are chosen indiscriminately.

These three traits define Unsolicited Bulk E-mail (UBE). If a fourth is added - that SPAM must be of a commercial nature - the resulting class of messages is referred to as Unsolicited Commercial E-mail (UCE).

Furthermore, ITU states that creating SPAM specific law can help focus enforcement efforts, strengthen norms against this behaviour, and close loopholes or uncertainties in existing laws that also apply to SPAM.

[13] This might differ according to the enforcement regime. In other words, is the private right of action available to individuals and/or corporations?. For instance, under CAN SPAM in the USA, there is no private right of action for individuals, but for ISPs. Typically, ISPs are not hold liable for SPAMmers' actions unless there is evidence that they are involved in helping, facilitating, commissioning or assisting in the SPAM. ISPs can take legal actions for the harm they suffered, and, if the private right of action is not available to individuals, then ISPs can sue SPAMmers on behalf of their customers to facilitate restitution of costs to damaged parties.

[14] *Source: The International Telecommunication Unions (ITU). On (www.itu.int/SPAM/)*

[15] Even with an opt-out regime, the assumption is that there is an assumed consent from the receiver and the message becomes unsolicited once the receiver opts out from receiving such messages.

## Technical Elements

The ITU suggests drafting regulations covering Internet communication generally rather than specifying applications (such as e-mail).

ITU further recommends that the legislation to be technology neutral in order to cater for the different media (whether wireless or wired) through which SPAM can originate.

## Consent

According to ITU:

Opt-in regimes focus on the means of obtaining, recording, and revoking consent, while opt-out regimes concentrate upon methods for indicating that one does not wish to receive messages, requirements for storing such preferences, and methods of enforcing this choice.

Any anti-spam regime with an opt-in system at its core is almost certain to be a more aggressive anti-spam regime than an opt-out system.

The lesson is that the strength of the sentiment in the law bears little correlation to the successful enforcement of that law. Choosing an opt-in versus an opt-out approach is not what matters if your end goal is to stop SPAM. The most effective anti-SPAM laws are action laws that focus on the problems prosecutors face and work to resolve them.

Most legal regimes, regardless of how they configure SPAM laws, prohibit messages that contain fraudulent, deceptive, or misleading information. Such bans typically target one or more of:

- The sender’s identity, e-mail address, or affiliation.
- The opt-out address used to refuse further communications.
- The material advertising or offering goods or services.
- The purpose of the message.
- The routing path of the message (including message headers).
- The message subject line.

## Commercial Elements

According to ITU:

- The initial decision for regulators in assessing SPAM is whether to differentiate among messages based on their content or purpose.[16]

[16] Many laws focus on messages that have commercial nature (for example Australia, USA), while other proposals seek to classify SPAM as any message (commercial and non commercial such as Malaysia) transmitted to recipients who have not requested it.

Focusing on the ‘Unsolicited’ nature of the message gives the regime more control over all types of messages being transmitted. Moreover, such decision targets the end users as it seeks to offer them more protection.

On the other hand, defining SPAM strictly as any message with ‘commercial’ nature will allow SPAMmers to send all kinds of non commercial messages causing annoyance and losses to various kinds of stakeholders without any fear being prosecuted or sanctioned.

An important aspect here is the legal context as well. For instance, the ‘freedom of speech’ and the rights afforded to political speech in some countries limit the ability of regulators to address messages of non commercial nature such as political and religious. The profit motivation for unsolicited commercial messages is often cited as a rational for focusing on this type of messages.

- A commonly accepted definition for the term Unsolicited Commercial Communications or Messages is shown below (Adapted from Australian and EU definitions): “Unsolicited commercial communications or SPAM, can thus be defined as unsolicited electronic communications sent in bulk over e-mail, mobile (SMS, MMS) and instant messaging services, usually with the objective of marketing commercial products or services.”

### Bulk

The ITU refers to the term Bulk as when the sender distributes a large number of essentially identical messages and those recipients are chosen indiscriminately. There are no recommendations regarding the number of messages considered as bulk.

ITU recommends considering the following elements to determine the characteristics of the bulk messages:

- Is the communication sent only to a small number of recipients (particularly those previously known to the sender) or to a large number of recipients?
- Does the list of recipients include fictitious or randomly generated addresses?

### Damage

The penalties for violating the dictates of regulations on SPAM generally fall under one of three categories: administrative penalties imposed by an enforcement entity, civil damages (actual or statutory) imposed by an adjudicating court, or criminal penalties imposed by a court in a criminal prosecution.

The level and type of penalties imposed in SPAM laws must reflect both a subjective judgment about the relative gravity of the harm in question and a more objective calculus about how to enforce effectively the relevant law.

Administrative penalties may be particularly useful as SPAM sanctions. Administrative agencies often use less formal and more rapid adjudication measures than court systems do; this reduction in the cost of enforcement can help improve compliance (assuming it is not offset by a corresponding increase in error rates in decision making). In addition, an agency with scope limited to data protection or consumer protection issues may be more focused and better equipped to deal with a problem like SPAM than an entity with broad law enforcement responsibilities.

### Requirements for Legitimate Messaging

ITU advises that using labelling of commercial e-mails, such as “ADV,” in the subject line of the message, would make it easier for SPAM filtering software to identify commercial e-mail and eliminate it.

Additionally, according to ITU analysis of existing SPAM laws:

- Unsubscribe requirements are particularly important for opt-out regimes since they provide the means by which recipients control whether they receive commercial messages. This method, though, is also useful for opt-in systems since it allows recipients to change their minds by revoking permission to communicate with senders.
- Most advice on spam cautions users against employing unsubscribe functions due to fears that senders will not comply with these requests and that attempting to unsubscribe will confirm that the recipient has received (and read) the message.

- Since there is a thriving market for e-mail addresses of recipients who actually open (and respond to) spam messages, unsubscribe requirements becomes more effective in opt-in schemes than in opt-out schemes; users are more likely to remember which senders they permit to transmit messages to them and thus can employ unsubscribe features for these senders while ignoring opt-out options from non-compliant senders.

### Exemptions or Restrictions

Jurisdictional elements in SPAM legislation define the conditions under which the law applies to an electronic message. At minimum, the states where the sender and the recipient are located would likely assert a jurisdictional interest in the message. Additional jurisdictions might be implicated based on the location of:

- The messaging service providers and Internet service providers involved;
- The computer used to transmit or to access the message;
- The entities responsible for or deriving benefit from the message’s contents;
- The organizations supervising or employing sender or recipient; and
- The developers of the software used to effect the communication.

### Address harvesting and Dictionary attacks

ITU recommends that drafters of a model of SPAM law ought to prohibit address harvesting and dictionary attacks, along with software tools specifically tailored to these purposes.

### Criminal or pornographic Content

According to ITU, SPAM holds the potential to fall under a number of different rubrics in terms of legal control, from computer misuse to false advertising to data protection to criminal fraud. Legal systems that implement SPAM legislation must consider, and hopefully specify, how these different elements will interact.

### In breach of fair trade

As mentioned in 3.1.2.9.

### Privacy

ITU states that regulators must resolve questions of responsibility and competence within their own borders with regulators of related issues such as criminal fraud, data protection, personal privacy, and computer misuse.

### ITU General SPAM - Related Legal Recommendations

According to ITU analysis of existing SPAM laws, these laws show considerable unity in defining the content they proscribe, despite the thorny challenge of widely divergent views about what constitutes prohibited expression.

Anti-SPAM laws around the world:

- Concentrate on content with a commercial, for-profit purpose.
- Prohibit communications that seek to defraud or mislead the recipient, that conceal the identity of the sender or the advertiser on whose behalf the message is transmitted, or that disguise information about the path that the message took in reaching a user.

- There is variation in whether laws apply only to one specific application (such as e-mail) or to on-line communication more generally.

A review of existing anti-SPAM laws suggests the following likely elements in a model law:

- Focus primarily on commercial content.
- Ban fraudulent or misleading messages.
- Prohibit concealing or falsifying a message's sender, advertiser, or routing information
- Draft regulations covering Internet communication generally rather than specifying applications (such as e-mail).

In March 2006 the ITU concluded that although all nations need anti-SPAM legislation "so that SPAMmers have nowhere to hide", a "more effective approach" would be to mandate establishment of enforceable codes of conduct by internet service providers, which would be held responsible for SPAM from their customers. Those codes would require ISPs to prohibit their customers from SPAMming and not to enter into peering arrangements with ISPs that do not accept similar codes of conduct.

Regulation of SPAM frequently overlaps with existing laws governing aspects of electronic communication or the content often found in SPAM. Regulators must decide how to align SPAM regulation with the following approaches:

- One Law or Many – Should the legal system adopt legislation specific to SPAM, or rely on regulation that addresses piecemeal the various aspects of its problems? Or can laws of general applicability, such as those that prohibit various forms of fraud or abuses of consumers, suffice?
- Rationalizing provisions – When the issue of SPAM falls under multiple, potentially conflicting or redundant regulations, how should this conflict be resolved?
- Reconciling theories – How can a particular approach to SPAM controls be aligned with the approaches to issues such as data protection, privacy, consumer protection, computer misuse, and fraud?

ITU clarifies that there are seven elements on which there is convergence in legislative provisions:

- Content: Focus on commercial / transactional messages, including advertising;
- Disclosure: Require the message to identify the sender and the advertiser;
- Truthfulness: Prohibit fraudulent or misleading content (including subject lines), and ban concealing or altering the routing path of the message;
- Addresses: Ban collection or generation of recipient addresses through address harvesting or dictionary attacks;
- Existing Relationship: Permit a sender to contact a recipient if the two parties have an established relationship, such as a prior transaction involving goods related to the subject of the message;
- Refusal: Mandate that recipients have the ability to unsubscribe from future communications from a sender, and that senders both respect this request and not

exchange the addresses of users who have opted out with others (except as needed to fulfil the request); and

- Liability: Employ a graduated[17] mixture of administrative, civil and criminal penalties.

ITU states that drafters of a model law ought to consider provisions that would:

- Require senders to provide recipients with a means to refuse, or unsubscribe from, future communications that is easy to use and inexpensive (preferably at no additional incremental cost);
- Require senders to respect unsubscribe requests and prohibit them from exchanging or selling addresses of recipients who unsubscribe;
- Prohibit address harvesting and dictionary attacks, along with software tools specifically tailored to these purposes; and
- Seek to standardize labelling requirements.

[17] Graduated refers to a system of penalties varying from administrative fines for minor offenses to criminal penalties for major or repeated violations.

## 4.2 ENFORCEMENT COOPERATION

### 4.2.1 OECD

Although OECD recommendations target mainly the OECD members, non-member economies are invited to take due accounts of the recommendations and collaborate with Member countries in its implementation.

Member countries are recommended to work to develop frameworks for closer, faster, and more efficient co-operation among their SPAM Enforcement Authorities that includes, where appropriate:

- Establishing a domestic framework.: Member countries should in this respect:
    - Introduce and maintain an effective framework of laws, SPAM Enforcement Authorities, and practices for the enforcement of Laws Connected with SPAM.
    - Take steps to ensure that SPAM Enforcement Authorities have the necessary authority to obtain evidence sufficient to investigate and take action in a timely manner against violations of Laws Connected with SPAM that are committed from their territory or cause effects in their territory. Such authority should include the ability to obtain necessary information and relevant documents.
    - Improve the ability of SPAM Enforcement Authorities to take appropriate action against (a) senders of electronic communications that violate Laws Connected with SPAM and (b) individuals or companies that profit from the sending of such communications.
    - Review periodically their own domestic frameworks and take steps to ensure their effectiveness for cross-border co-operation in the enforcement of Laws Connected with SPAM.
    - Consider ways to improve redress for financial injury caused by SPAM.
- Improving the ability to cooperate: Member countries should improve the ability of their SPAM Enforcement Authorities to cooperate with foreign SPAM Enforcement Authorities. Member countries should in this respect:
    - Provide their SPAM Enforcement Authorities with mechanisms to share relevant information with foreign authorities relating to violations of their Laws Connected with SPAM upon request, in appropriate cases and subject to appropriate safeguards.
    - Enable their SPAM Enforcement Authorities to provide investigative assistance to foreign authorities relating to violations of their Laws Connected with SPAM upon request, in appropriate cases and subject to appropriate safeguards, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying persons or things.
    - (Designate a contact point for co-operation under this Recommendation and provide the OECD Secretariat with updated information regarding their Laws Connected with SPAM and the SPAM Enforcement

Authority designated as the contact point. The OECD Secretariat will keep record of this information and make it available to interested parties.

- Improving procedures for co-operation: Before making requests for assistance as foreseen in the previous paragraphs, SPAM Enforcement Authorities should:
  - Proceed to some preliminary investigative work to determine whether a request for assistance is warranted, and is consistent with the scope and priorities set forth by this Recommendation.
  - Attempt to prioritise requests for assistance and, to the extent possible, make use of common resources such as the OECD Website on SPAM, informal channels, existing international networks and existing law enforcement co-operation instruments to implement this Recommendation.
- Cooperating with relevant private sector entities.
  - SPAM Enforcement Authorities, businesses, industry groups, and consumer groups should cooperate in pursuing violations of Laws Connected with SPAM. In particular, SPAM Enforcement Authorities should cooperate with these groups on user education, promote their referral of relevant complaint data, and encourage them to share with SPAM Enforcement Authorities investigation tools and techniques, analysis, data and trend information.
  - Member countries should encourage co-operation between SPAM Enforcement Authorities and the private sector to facilitate the location and identification of SPAMmers.
  - Member countries should also encourage participation by private sector and non-member economies in international enforcement co-operation efforts; efforts to reduce the incidence of inaccurate information about holders of domain names; and efforts to make the Internet more secure.

### 4.2.2 ITU

International cooperation on enforcement is essential in order to ensure the effectiveness of anti-SPAM rules. In other words, it must be possible to trace back SPAMming activities and prosecute SPAMmers, regardless of national borders.

As a pre-requisite, national legislation could facilitate information sharing and mutual assistance between competent authorities in different countries. Appropriate bilateral and/or multilateral cooperation would enable appropriate information sharing and mutual assistance on specific SPAM cases.

The choice of the international instrument(s) to do this may depend on various factors. However, all organizations can in any event promote such cooperation on enforcement within the limits of their competence.

Certain countries, including some EU Member States, have concluded cooperation agreements (e.g. Memoranda of Understanding) to facilitate such cooperation[18]. These documents generally

[18] Examples of existing MoUs and International agreements are depicted in Appendix B.

call upon participating parties to produce their 'best efforts' to cooperate with each other on issues such as building evidence, user education, new SPAMming activities, training, etc.

At the multilateral level, some countries already participate actively in international discussions (e.g. ITU, OECD, APEC, EU), where work on SPAM has started. Active participation in this work of all countries with originators and recipients of SPAM is encouraged.

### 4.2.3 LAP[19]

The London action plan comprises of government and public agencies from 27 countries responsible for enforcing laws concerning SPAM that met in London to discuss international SPAM enforcement cooperation. At this meeting, a broad range of SPAM enforcement agencies, including data protection agencies, telecommunications agencies and consumer protection agencies, met to discuss international SPAM enforcement cooperation. Several private sector representatives also collaborated in parts of the meeting:

1. The participating government and public agencies (hereinafter "Agencies"), intend to use their best efforts, in their respective areas of competence, to develop better international SPAM enforcement cooperation, and intend to use their best efforts to:
    - Designate a point of contact within their agency for further enforcement communications under this Action Plan.
    - Encourage communication and coordination among the different Agencies that have SPAM enforcement authority within their country to achieve efficient and effective enforcement, and to work with other Agencies within the same country to designate a primary contact for coordinating enforcement cooperation under this Action Plan.
    - Take part in periodic conference calls, at least quarterly, with other appropriate participants to:
        - ➢ Discuss cases.
        - ➢ Discuss legislative and law enforcement developments.
        - ➢ Exchange effective investigative techniques and enforcement strategies.
        - ➢ Discuss obstacles to effective enforcement and ways to overcome these obstacles.
        - ➢ Discuss undertaking, as appropriate, joint consumer and business education projects addressing problems related to SPAM such as online fraud and deception, phishing, and dissemination of viruses. Such projects could include educational efforts addressing conditions facilitating the anonymous delivery of SPAM, such as the use of open relays, open proxies and zombie drones.
        - ➢ Participate as appropriate in joint training sessions with private sector representatives to identify new ways of cooperating and to discuss SPAM investigation techniques.
    - Encourage dialogue between Agencies and appropriate private sector representatives to promote ways in which the private sector can support

[19] *Source: London Action Plan (LAP). On (www.londonactionplan.com/)*

Agencies in bringing SPAM cases and pursue their own initiatives to fight SPAM.

- Prioritize cases based on harm to victims when requesting international assistance.
- Complete the OECD Questionnaire on Cross border Enforcement of Anti SPAM Laws, copies of which may be obtained from the OECD Secretariat.
- Encourage and support the involvement of less developed countries in SPAM enforcement cooperation.

The participating Agencies intend to keep information shared in the context of this Action Plan confidential when requested to do so, to the extent consistent with their respective laws. Similarly, the participating Agencies retain the right to determine the information they share under this Action Plan.

2. The participating private sector representatives (whether as a group or through its members) intend to use their best efforts to develop public private partnerships against SPAM and to:

   - Designate a single SPAM enforcement contact within each organization, which would coordinate with SPAM enforcement agencies on requests for enforcement related assistance.
   - Work with other private sector representatives to establish a resource list of individuals within particular sectors (e.g., Internet service providers, registrars, etc.) working on SPAM enforcement.
   - Participate as requested and appropriate in segments of the periodic conference calls described in paragraph A.3 above for the purpose of assisting law enforcement agencies in bringing SPAM cases. (Because some calls will be focused solely on law enforcement matters, private sector representatives will participate only in selected calls.) In these conference calls, the participating private sector representatives intend to use their best efforts to:
     - ➢ Report about:
       - i. Cases involving SPAM or related matters.
       - ii. New technology and trends in email and SPAM.
       - iii. New ways of cooperating with Agencies.
       - iv. Obstacles to cooperation with Agencies and within the private sector.
       - v. General data on SPAM and on line fraud as an early warning mechanism for Agencies.
     - ➢ Assist as appropriate in training sessions on subjects such as the latest SPAM investigation techniques to help Agencies in investigating and bringing SPAM cases.

In order to prevent inappropriate access to information, a private sector representative may be excluded from participating in all or a portion of the periodic conference calls described above if a participating Agency objects.

- Work cooperatively with Agencies to develop the most efficient and effective ways to frame requests for information. For this purpose, each participating private sector representative intends to use best efforts to compile written responses to the following questions:
  - What kind of information do you provide about potential SPAMmers to domestic law enforcement agencies and under what circumstances?
  - What kind of information would you provide about potential SPAMmers to foreign law enforcement agencies and under what circumstances?
  - How do you recommend that SPAM enforcement agencies submit requests for assistance to you?

3. In order to begin work pursuant to this Action Plan, the U.K. Office of Fair Trading and the U.S. Federal Trade Commission intend to use best efforts to:

   - Collect and disseminate information provided pursuant to this Action Plan, including points of contact, notifications from new Participants of their willingness to endorse this Action Plan, and responses to questionnaires, in cooperation with the OECD.
   - Set up the conference calls mentioned in paragraph A.3.
   - Provide a contact for further communications under this Action Plan.

   The participating Agencies expect that this procedure may be modified at any time.

4. This Action Plan reflects the mutual interest of the Participants in the fight against illegal SPAM. It is not intended to create any new legally binding obligations by or amongst the Participants, and/or require continuing participation.

Participants to this Action Plan recognize that cooperation pursuant to this Action Plan is subject to their laws and their international obligations, and that nothing in this Action Plan requires the Participants to provide confidential or commercially sensitive information.

Participants in this Action Plan intend to use best efforts to share relevant findings of this group with the OECD SPAM Task Force and other appropriate international groups.

Additional Agencies, and private sector representatives as defined below, may endorse and take part in this Action Plan as long as no Agency that has endorsed this Action Plan objects.

"Private sector representatives" invited to participate in this Action Plan include financial institutions, Internet service providers, telecommunications companies, information security software providers, mobile operators, courier services, commercial mail receiving agencies, industry membership organizations, consumer organizations, payment system providers, credit reporting agencies, domain name registrars and registries, and providers of alternative dispute resolution services.

## 4.3 INDUSTRY DRIVEN ACTIVITIES

### 4.3.1 OECD

OECD listed some recommendations that Business and Industry Advisory Committee (BIAC) proposes. The following Best Practices for ISPs and Network Operators are an important tool in combating SPAM. These Best Practices and any additional measures are voluntary, and in all cases precedence is given to applicable legal and regulatory frameworks. In any given national jurisdiction, each of the Best Practices is understood to be recommended only if it is not in contradiction with existing national legislation.

Implementation of these Best Practices and any additional measures will vary, depending on the technical configurations of particular providers'/operators' networks, and their specific business needs and challenges. We note that flexibility in the implementation of these Best Practices and any additional measures is the key to achieving their broad and meaningful adoption by service providers of all sizes. Given the rapid pace of technological change, the Best Practices will be periodically reviewed and updated.

The OECD has some recommendations of its own with the main purpose of reducing SPAM, as follows:

- Governments and regulators should support the development of ISP codes of practice that complement and are consistent with legislation.
- Governments should encourage industry associations to develop such codes and adopt best practices where they are in the public interest and do not impose undue financial and administrative burdens on participants.
- Legislation could also provide a comprehensive framework to support the activities of ISPs to block or limit the circulation of SPAM e-mail.
- ISPs should be able to take appropriate and balanced defensive measures to protect their networks, and should be allowed to take legal action against SPAMmers. Similar results could be achieved through appropriate contractual provisions between ISPs and users.
- "More effective approach" would be to mandate establishment of enforceable codes of conduct by internet service providers, which would be held responsible for SPAM from their customers. Those codes would require ISPs to prohibit their customers from SPAMming and not to enter into peering arrangements with ISPs that do not accept similar codes of conduct.
- Direct Marketers should adopt and effectively implement a code of conduct using best practices for electronic marketing, which include marketing messages sent by e-mail, instant messaging, or mobile.

### 4.3.2 ITU

The ITU has issued a document targeting the industry, that is, the service providers, direct marketers, and software makers urging them to adapt their practices in order to combat the ever increasing threat of SPAM. This should be promoted across the globe, in particular since many companies operate on a multinational basis.

This concerns not only contractual practices (e.g. adaptation of terms and conditions for use of servers) but also marketing practices.

Self-regulatory tools (e.g. codes of conducts) should be encouraged and systematically improved with experience. Industry should also be encouraged to share their expertise and best practices, both across industry branches (e.g. direct marketers with ISPs, and those players with software manufacturers), and across countries and regions in the world.

Improved cooperation on enforcement between industry and enforcement authorities should also be promoted, in particular to trace SPAMmers and provide evidence that will be used to build investigation and prosecution.

### 4.3.3 GSM ASSOCIATION[20]

The primary goals of the GSM Association (GSMA) are to ensure mobile phones and wireless services work globally and are easily accessible. It helps its members develop and launch new services, ranging from mobile instant messaging to video sharing to mobile Internet access, which will work across networks and across national boundaries.

#### Awareness

A section of the website has been dedicated to general information about SPAM, it contains a definition, what common types of SPAM you may be receiving, and how to minimise the impact of mobile phone SPAM. (http://www.gsmworld.com/using/security/SPAM.shtml).

#### Industry Driven Initiatives

The GSMA developed a Mobile SPAM Code of Practice along with its member operators. It has been devised to protect the secure and trusted environment of mobile services to ensure customers receive minimal amounts of SPAM sent via SMS and MMS. The Code takes a firm stance on how to deal with mobile SPAM messages that are either fraudulent or unsolicited commercial messages. To support this initiative the GSMA is encouraging member operators to sign-up to the Code and for governments and consumer associations to support industry in its endeavors.

The code is voluntary and applies specifically to three types of messages; commercial messages sent to customers without their consent, commercial messages sent to customers encouraging them directly or indirectly to call or send a message to a premium rate number and bulk unlawful or fraudulent messages sent to customers. The main purpose of the code was to limit the amount of SPAM being received by end users, provide a common basis for operators to work together to combat mobile SPAM and share best practices, and encourage industry assistance with the respective governments.

Under the Code, the mobile operators that are signatories commit to:

- Include anti-SPAM conditions in all new contracts with third party suppliers;
- Provide a mechanism that ensures appropriate customer consent and effective customer control with respect to mobile operators' own marketing communications;
- Work co-operatively with other mobile operators, including those who are not signatories to the Code;

[20] *Source: http://www.gsmworld.com/*

- Provide customers with information and resources to help them minimise the levels and impact of mobile SPAM;
- Undertake other anti-SPAM activities, such as: ensuring that an anti-SPAM policy is in place that prohibits the use of the mobile network for initiating or sending mobile SPAM, and adopting GSMA recommended techniques for detecting and dealing with the international transmission of fraudulent mobile SPAM; and
- Encourage governments and regulators to support industry.

### 4.3.4 Mobile Marketing Association[21]

The Mobile Marketing Association (MMA) members include agencies, advertisers, hand held device manufacturers, carriers and operators, retailers, software providers and service providers, as well as any company focused on the potential of marketing via mobile devices. Privacy Advisory Committee members Carat Interactive, Cingular Wireless, Procter & Gamble, PocketChoice. The Weather Channel, and VeriSign developed this Code of Conduct.

#### Choice

Consumers must opt-in to all mobile messaging programs. Consumers may opt-in to a program by sending a text message, calling a voice response unit, registering on a website, or through some other legitimate paper-based method; they opt-in for a specific program only.

Choice doesn't carry forward unless the consumer is part of a brand loyalty program whose opt-in registration clearly provides for on-going communications. Even then, the consumer's desire to participate must be validated at the beginning of a new messaging program. Segmentation-based marketing (by interests, demographics, etc.) and location-based marketing is prohibited unless the consumer clearly opted-in to receive the campaigns by giving personally identifiable information that is verifiable with their identity.

#### Control

Consumers must also be allowed to easily terminate -- opt-out -- their participation in an ongoing mobile messaging program through channels identical to those through which they can opt-in to a given program. Programs with multiple message strings must provide an opt-out option for each message.

#### Customization

As mobile messaging campaigns are most effective when appropriately targeted, consumers could be asked to provide demographic, preferences and other information. All "follow on" communications targeted at an existing opt-in universe should be encouraged to use this data to optimize message volumes, redemption rates, and return-on-investment -- plus restrict communications to those categories specifically requested by the consumer.

#### Consideration

The consumer must receive and/or be offered something of value to them in return for receiving the communication. Value may be delivered in the form of product and service

[21] *Source: http://mmaglobal.com/*

enhancements, reminders, sweepstakes, contests, information, entertainment, discounts or location-based services.

### Constraint

The marketer, content provider, or aggregator must provide a global "throttling mechanism" capable of managing the number of messages received by an individual consumer. The purpose of the throttle is to effectively manage and limit mobile messaging programs to a reasonable number of programs, defaulted to a maximum of 2 new campaigns per week (One campaign may have one initial opted-in communication followed by several two-way communications initiated by the consumer as part of that one campaign; i.e. a trivia game). Consumers will have the option to override the throttle through an additional Opt-in available through the standard channels.

### Confidentiality

Align with TRUSTe with specific provisions on not renting, selling or sharing personal information about consumers participating in programs delivered through its platform with other people or nonaffiliated companies except to provide the products and services requested.

Aggregated, non-personal, non-individual information might be shared collectively with partners for research purposes only. All customers should be subjected to the terms and conditions of a privacy policy that meets TRUSTe's example.

## 4.4 TECHNICAL SOLUTIONS

### 4.4.1 OECD

General Recommendations, with regard to Anti-SPAM Technical Solutions, provided by OECD include:

- Judicious application of technology should be the backbone of any approach that aims to defeat SPAM.
- One should be aware that none of the technologies discussed in the following will act as a "silver bullet" or one-stop solution to the problems created by SPAM. Instead, it should be recognized that all of the technologies are complementary and will be most effective when implemented in conjunction with each other.
- The integration of a number of technologies is necessary to reduce the harmful impact of SPAM on a system.
- Internet service providers and network operators can contribute to combating SPAM on two different fronts: on the technological side, they may develop and apply technology solutions to limit or block not only the receiving, but directly the sending of SPAM messages. On the operational side, they are in the position to implement a code of conduct for ISPs and to impose on their customers Acceptable Use Policy (AUPs) forbidding SPAM
- Given the link between SPAM and network security, providers, besides using filters to block the reception of SPAM, should also improve security on their network, to avoid becoming a source of SPAM. Many providers hold the view that the problem of botnets and zombies can be solved, or at least limited, by implementing security best practices, applying AUPs and educating users to employ available tools to protect their computers.
- The Anti-SPAM Technical Alliance (ASTA), a collaborative effort between some of the leading Internet providers and the Internet community, active until 2004, was created to establish technical and non-technical solutions for handling unsolicited commercial e-mail. The alliance created a technology and policy proposal., which was issued in June 2004, and included a series of best practices and technical approaches that ISPs should adopt in order to control abusive traffic thus reducing the chances for a SPAMmer to (mis)use their servers to send unsolicited messages. These techniques are based on .Good Neighbour policies, i.e. ISPs are responsible for controlling the traffic they originate.

  The ASTA Technology and Policy proposal included a series of best practices and technologies that ISPs should implement to help secure the e-mail infrastructure and bring about increased accountability[22].

However, the document recognises that technical solutions are not the solution to the SPAM problem, and acknowledges that provisions must be flexible and ready to change to adapt to the rapidly evolving Internet environment and its vulnerabilities. For this reason governments are refraining from imposing technological solutions on ISPs, and ISPs associations and alliances prefer to concentrate more generally on agreeing on best practices and objectives, rather than

[22] The Code of conduct can be accessed at: http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf

setting up specific rules. A typical example of this approach is the Code of Conduct adopted by the Messaging Anti-Abuse Working Group (MAAWG)[23], an organization now including almost all former ASTA members, and continuing the technical work initiated there.

Within Operation SPAM Zombies about 30 economies were engaged in contacting ISPs around the world to urge them to:

- Block port 25, except in certain circumstances.
- Apply rate-limiting controls for e-mail relays.
- Identify computers that are sending atypical amounts of e-mail, and take steps to determine if the computer is acting as a SPAM zombie; when necessary, quarantine the affected computer until the source of the problem is removed.
- Give customers plain language advice. And
- Point customers to tools to remove zombie code.

According to OECD, there is no universal consensus, however, on the first measure, i.e. blocking port 25. A number of ISPs, while willing to contribute to co-operative initiatives are reluctant to take the responsibility for monitoring and fixing compromised computers in their networks.

## Anti-SPAM Technologies

The following are types of anti-SPAM technologies that are designed to fight SPAM. While some of them aim to prevent certain types of behaviour which pose a threat to security and fail to respect the resources of the platform to which mail is sent or simply do not comply with the accepted rules for sending electronic messages, and some of them are depended on the location of the rule.

In the following two sections, both, the ones which do not comply with accepted rules for sending messages and the ones which are depended on the accepted rules for sending messages will be described:

### Anti-SPAM Techniques that do not comply with rules for sending messages

#### 1 Authentication of electronic mail

The first comment that needs to be made is that mail authentication methods fall into the category of rules, which, although they help in the fight against SPAM, do not constitute specific anti-SPAM technologies.

#### 2 SPF and/or Sender-ID

OECD toolkit mentioned that SPF and Sender-ID can be used to test whether an e-mail server is authorized to send on behalf of a given domain. This is done by publishing a record in the Domain Name System (DNS), which lists the authorized e-mail servers for a domain. The two techniques primarily differ in the choice of the identity tested.

[23] The MAAWG Code of Conduct can be accessed at: http://www.maawg.org/about/CodeofConduct.pdf

## 3 DKIM /or META

DKIM and Message Enhancements for Transmission Authorization (META) are used to authenticate the sender domain by means of a cryptographic signature automatically added by the e-mail server. At present, the immediate practical benefits are very low since few domains sign their messages. Furthermore, administrators will note that these three techniques are not yet based on a stable standard.

## 4 Existence of the sender's domain and eliciting a response

Many SPAMmers send mail with a non-existent sender's address. A rule can be used to refuse these messages, such as the Postfix directive reject_unknown_sender_domain or the j-chkmail directive BadMX. Another possibility is to verify the validity of the record for the incoming server (MX) for the domain given in the "from" field of the message.

## 5 Existence of a Pointer Record (PTR)

A PTR record of the DNS can be used to translate the IP address of the sender's server into a name, although without necessarily checking that this name is consistent with the sender's domain.

## 6 Blacklists/Whitelists

Traditional filtering as well as tracking complaints across user communities can ultimately lead to whitelists of acceptable senders and blacklists of suspected SPAMmers. The whitelist/blacklist approach is often a too drastic solution to be acceptable by most users. Whitelists are time-consuming to create and will require continual updating. Blacklists require similar monitoring. All lists need mechanisms and procedures for updating to address false positives and fraudulent complaints to a listing. Spoofing and open relays can also create issues related to the appearance that mail has originated from a source.

## 7 Address of the sending server treated as either dynamic or residential

This is a particular form of blacklist in which the criterion for addition to the list is the fact that the IP address being blocked corresponds to the machine of an individual subscriber to an ISP and not to the mail server of an organisation. The idea is that an ordinary subscriber does not send mail directly in SMTP, but passes through the PTA of his provider. This typically means the machine being blocked is directly sending SPAM messages from a SPAMmer, or more commonly that the messages are being sent without the owner's knowledge (i.e. the machine has been compromised and turned into a zombie in order to send the messages).

The lists of such addresses are not always reliable since most of them have been compiled using heuristics, such as the presence of .adsl. in the name of the machine. Managing such lists is also resource intensive.

In contrast, some of these lists, notably those compiled by the server using them, can be used to distinguish between servers authorised for a domain and the residential lists. Moreover, some domains publish the ranges of residential addresses for their domain.

This test can be seen as discriminating between pure consumers and providers. The latter consider legitimate the policy by which the owner of a domain refuses to connect his machines to residential addresses, as these are currently the main source of SPAM. Consumers however argue that SPAM exists and the freedom to use e-mail must be protected.

## 8 Filtering

Filtering is the most common technical anti-SPAM technology. The main benefits of filters are the ease of implementation and the flexibility that users have in deciding which messages should be treated as SPAM. The following are type's filters for combating SPAM:

A. Heuristic filters

These filters are based on the principle of testing for the presence in the message of certain typical features of SPAM, such as the exclusive use of HTML or the type of customer to whom the mail is sent. The test is weighted through a learning process based on a set of known SPAM mails and a set of mails known to be legitimate.

B. Keyword filters

These are binary filters that search for a keyword ("Viagra" etc.). The risk of false positives is very high and the ability to avoid these by spacing, alternate characters and misspelling is also substantial.

C. Summary or fingerprint filters

Fingerprint filters, such as Razor, construct a fingerprint of the message submitted to them and indicate whether it has already been identified as SPAM. There are many false negatives because a number of types of SPAM mail are not identified even when the server scans them with Razor. Furthermore, the message sometimes varies sufficiently for it to generate a different fingerprint. One solution to this problem is to delay the mail (as greylisting does). They generate few false positives.

D. Bayesian filters

The principle on which the Bayesian filter works is to prime its engine by examining a set of known SPAM e-mails and a set of e-mails known to be legitimate, then after teaching itself the vocabulary used by SPAMmers from this known list it will use Bayesian probabilities to calculate whether a message is SPAM. In the case of a group filter, the learning is usually conducted by the system administrator.

E. Behavioural filters

This type of filter examines the behaviour of the remote server, such as the number of mails sent by unit of time. Rate limiting is one example of this type of filtering. The idea is that ordinary mails are only sent individually or in very small numbers and SPAM mails are sent in very large batches.[24]

## 9 HELO/CSV

A sending computer identifies itself by name to a receiving computer at the beginning of each SMTP transaction. The SMTP command the sending computer uses to identify itself by this name to the receiving computer is called the "EHLO" or "HELO" command. Certified Server Validation (CSV) is a service that provides a mechanism for a mail-receiving server to assess a mail-sending server. It builds upon the existing practice of service providers that accredit the networks from which sending systems are connecting.

## 10 Greylisting

This is the deliberate sending of an SMTP 4xx error code (a temporary error as opposed to a 5xx definitive error, see RFC 2821) when encountering a new sender. The latter, if it is a normal MTA, will try again later (usually 15 minutes later) and its message will then be accepted. Most SPAM software programs do not make multiple send attempts. This technique is highly effective and blocks all SPAM mails that are not sent through an open relay or by the MTA of a provider. It prevents receipt of certain messages from poorly configured servers and lends itself particularly well to be used in conjunction with a whitelist.

## 11 Tokens/passwords

The aim of these techniques is to include a password in the address to which the e-mail is sent or to use a challenge/response system such as the Turing test. The SPAMmer's software will not know this password and will be unable to pass the test.

## 12 Other techniques

There are various techniques that mostly are experimental and insufficiently tested, and they are Envelope tests (BATV, SES), Certification of Bulk Mails, Micro Payment System, PGP Signature, System Configuration, Anti-SPAM Tools and Anti-Spyware tools. (For more explanation on these tools/technologies please refer to the OECD toolkit)

[24] For OCR (Optical Character Recognition), the gibberish or nonsense text included with image spam very quickly becomes "red-flag" text by a Bayesian filter. An image with little or no accompanying text is also a red flag, because almost all legitimate mail that contains images also includes a reasonable amount of body text. Normal connection-level techniques such as greylisting and DNS-based RBLs continue to be effective against image spam as well. Resorting to using OCR tools to extract the text from an image spam for analysis was met with limited success. The state-of-the-art in OCR is not very advanced. Furthermore, OCR tools are not designed to extract text from an image that is actively being manipulated by an adversary. Spammers have reacted to OCR tools by obfuscating the text in the images they send. The obfuscated text is still relatively easy for humans to recognize, but very difficult for OCR tools to extract. In addition to the accuracy problem, OCR is very compute-intensive and can greatly slow down a content filter.

Overall, the utility of any tool(s) will be dependent on the needs, technical ability and the infrastructure of the user of the same tool. Tools are meant to be deployed at different parts across the system and for differing purposes. Users will have to consider their needs and strategies of defense in depth as they choose and deploy anti-SPAM tools. Tools themselves vary in maturity, efficacy, reliability and deployment. Some tools are more prone to false positives some are more effective in certain areas and some have greater overhead in terms of cost, infrastructure, bandwidth/capacity and needed technical expertise. A number of these factors have been listed for consideration, but user will have to gauge tools in the specific context of their contemplated application.

## Anti-SPAM Techniques that are depended on the accepted rules for sending messages

### 1 Rejection in the SMTP session

The interest in such rejection lies in not taking charge of the electronic message, whose distribution remains the responsibility of the remote server, which has been advised of the situation. In addition it saves bandwidth capacity, firstly because the message is not received and secondly because the remote server will not have to send DSNs (Delivery Status Notification, the message generated in response to a rejection, see RFC 3461) that the message might generate. The task of issuing such a non-delivery message is transferred to the sender.

### 2 Silent rejection

This method often confounds regular users who expect their e-mail to be delivered or at least to be told that it has been rejected. The “deliver or advice” alternative is a cardinal principle of e-mailing, but one which will probably have to be abandoned due to the number of “joejobs”[25].

### 3 Rejection by sending a DSN (Delivery Status Notification or “bouncing”)

This is the method traditionally used in Internet e-mailing. However, due to the presence of “joejobs”, there is a risk of penalizing innocent senders, as may be seen with the anti-virus programs which mistakenly send DSNs.

### 4 Delivery to a SPAM box

When few messages are blocked on entry to the platform, the SPAM box can contain very large volumes of messages, which can discourage users from reading it. The message is not destroyed, but the user is given an opportunity to remedy false positives.

### 5 Marking

The server takes no decision but simply places a note on the e-mail. This technique gives the user full control, but will also force the user to download SPAM mail. Note that an e-mail service provider can offer the user the choice of simply marking the e-mail or delivering it to the SPAM box. It is relatively simple to manage.

[25] a spam attack using spoofed sender data and aimed at tarnishing the reputation of the apparent sender and/or induce the recipients to take action against him.

### Overall View

Overall, the previous discussion was about various anti-SPAM technologies and their capabilities presently available, as well as of the methods to be employed when SPAM is received. Any attempt to combat SPAM effectively must involve the sensible administration of a number of these technologies in concert. None of the above methods will be entirely successful in isolation. When a number of anti-SPAM technologies are effectively used in collaboration with one another, the effect can to drastically reduce the level of SPAM impacting a system.

### 4.4.2 ITU

#### Technical Measures

To succeed in controlling SPAM, regulatory efforts through legislation and rulemaking must be accompanied by – or at least coordinated with – technological reform measures that reduce the incidence of these unwanted messages while minimizing the impact on legitimate messages. These technical methods fall roughly into four categories: filters, cost-shifting, authentication, and security.

#### Filters

Filtering attempts to detect and block or quarantine SPAM messages. Filters can be installed at many layers of the network, for instance by e-mail service providers, Internet service providers, and individual users. Filters search messages for characteristics that indicate SPAM, such as a fictitious domain in the message's return address or the presence of keywords such as "Viagra", or close variants such as "Vi*gra," in its body. More sophisticated filters employ techniques such as Bayesian statistical analysis that use probabilistic assessment of words in a message and that are capable of refinement with increased accuracy over time. Filtering can prevent end users from even seeing SPAM messages, and by reducing the risk that they (or their children) might be exposed to offensive content such as graphic advertisements for pornography. Filters are widely used both by ISPs and by individuals at the client level to reduce e-mail SPAM. While most filters are produced by private companies or developers, SPAM regulators may be authorized to contribute to or to support such tools.

Filters can be augmented using two additional tools: "blacklists" and "whitelists". Blacklists compile data about known SPAM sources and senders. This enables service providers to scrutinize or block e-mail traffic from these sources. Blacklists are generally compiled and maintained by private companies or organizations. Though blacklists can be valuable in blocking defined sources of SPAM, their use implicates questions about standards for being added to and removed from a list, the speed of updates, and the power such lists confer on the compiler. In addition, SPAMmers have begun to adopt new techniques, such as routing messages through ISP servers that reduce blacklists' effectiveness.

Whitelists perform the opposite role as they validate certain senders as sources of legitimate messages. Therefore, messages from these senders either bypass filtering entirely or are scrutinized at a much reduced level. Simple whitelist techniques, for example, allow senders listed in a user's address book to bypass filters installed by that end user. More advanced methods, such as "bonded sender" or "payment at risk" programs, incorporate monetary guarantees by senders. Payment at risk penalizes a sender financially if a message is SPAM or if the recipient is dissatisfied with it. Bonded sender programs require senders to post a monetary guarantee of their e-mail advertising before they are permitted to bypass SPAM filters. Whitelists simplify filtering by classifying certain messages as "low risk," meaning that it's highly unlikely they are SPAM. However, whitelists impose costs on senders that may have negative distributional consequences and require the participation of filtering entities to be effective. Whitelists are also ineffective if a message falsely purports to be sent by a sender in the whitelist or is sent from a hijacked computer in the whitelist.

While filtering is an important tool in addressing SPAM, it suffers from three primary drawbacks: overblocking, underblocking, and reduced control. Overblocking by filters removes legitimate messages as well as SPAM. The level of overblocking depends both on the filter used and its implementation. A study by e-mail marketing firm Return Path found that seventeen per cent of permission-based messages (whose recipients consent in advance to receive the e-mail) were blocked by SPAM filters. This over-inclusiveness can also occur when users attempt to send messages if their service provider implements outbound SPAM filtering. Overblocking is harmful because it prevents recipients from accessing (or sending) desired, legitimate messages and because it undermines their confidence in the reliability of e-mail as a communications medium.

Underblocking occurs when filters fail to detect or to remove messages that are SPAM. This under-inclusiveness results both from the arms race between SPAMmers and filters – for example, SPAMmers have begun including unusual but innocuous words in messages to evade Bayesian filters – and from the difficulties inherent in analyzing the content and intent of e-mail. Underblocking demonstrates that technical methods are only a partial solution to SPAM.

Finally, SPAM filters implicate important questions of control over receiving and sending content. Filters implemented at the service provider level decrease the control that end users have over what types of messages they receive. For example, an individual user might prefer to receive certain unsolicited messages, such as messages advertising credit card offers, and such messages may be blocked as SPAM from his ISP. Alternately, a user might decide the risk of not receiving even a single incorrectly blocked message is unacceptable. Conversely, filtering implemented by end users may be updated less frequently and configured less skillfully if users are not technologically savvy. This is particularly important regarding SPAM that contains viruses, worms, or bots.

## Cost-Shifting

Cost-shifting proposals seek to reduce the volume of SPAM by increasing the sender’s costs, either in money or in computing time, to transmit each message. The goal is to alter the unusual economics of SPAM, in which the sender incurs almost no cost to send messages while the costs to transport the message, store it, and delete it are borne by the recipient and third parties such as ISPs. In addition, senders can often transmit a single message that is delivered to many recipients. Thus, since the advertising item itself does not need to be printed and distributed as a separate piece for each recipient, sending large numbers of solicitations does not incur increasing costs. The result is that fractional response rates that would be a disaster in traditional direct marketing become profitable on the Internet.

E-stamp solutions propose to modify the electronic mail infrastructure to either allow or require a monetary payment for each message sent. Even a tiny increase in the costs of sending an individual message would make mass mailings of tens of millions of messages economically unfeasible. Commercial mass marketers accustomed to traditional response rates in other media should not be deterred by a small charge to send marketing material. In addition, many E-stamp proposals provide a base daily level of free messages (such as a hundred per day at no charge) to individual users, so few senders would incur any additional cost.

However, E-stamp proposals suffer from a number of drawbacks. As many observers have noted, such an increase in cost would prove crippling to many developing nations that are in the early stages of adopting new information and communications technologies infrastructures. All of these proposals not only require major changes to the existing electronic mail infrastructure, but also penalize everyone who sends e-mail, not just SPAMmers. Since any additional cost imposed on each message cost must be a fixed, relatively small amount, this form of cost-shifting is unlikely to deter the most harmful forms of SPAM -- those seeking to defraud the recipient -- that offer the sender relatively large rewards. In addition, while a penny per message charge may be negligible to a large developed-country corporation, it may be a significant amount of money in the developing world (in which case a pay-to-send system could worsen the digital divide). Developing and deploying the infrastructure for every mail server and client in the world to handle micro-payments in world currency appears daunting at best and impossible in any near-term time frame. Finally, even at small per-message amounts, the huge amount of daily e-mail traffic implicates dollar amounts that create a sizeable opportunity for fraud and electronic theft from any system of cash E-postage.

As an alternative to requiring a cash payment for each message, several anti-SPAM proposals would require the sending computer to compute a complicated numerical puzzle and return the correct answer to the recipient before the recipient would accept the message. This creates a small delay in sending each message. While invisible to most users, such methods would make it impossible for a SPAMmer to send tens or hundreds of millions of messages a day from a few computers connected to the Internet. Because computing solutions do not involve money transfers, the issues of currency conversion, fraud, and relative value plaguing E-stamp solutions are minimized.

However, computing solutions still require major changes to the e-mail infrastructure and burden all senders, not just undesirable ones. Much of the value of e-mail derives from its low cost. Many legitimate senders, including businesses, government agencies, private organizations, and independent newsletter authors, send large quantities of electronic mail. Much of this traffic is not income-generating but informational; for example, the low cost of sending e-mail has enabled incremental package tracking, frequent government informational updates, and a host of special-interest electronic newsletters from non-commercial and non-profit entities. Changing the economics of bulk e-mail could drastically curtail the free flow of information that characterizes the Internet. Finally, much of the current SPAM problem originates from computers that have been hijacked by SPAMmers. If SPAMmers can employ other users' resources to transmit messages, computing cost solutions are unlikely to deter unwanted messages while placing a severe burden on legitimate senders.

## Authentication

Any legal solution to regulating SPAM, even one well-harmonized among different regimes, is challenged by the difficulty of holding violators accountable. The Simple Mail Transport Protocol (SMTP) used to transmit Internet e-mail does not authenticate senders, allowing violators of messaging regulations to hide their identities behind false header information, hijacked zombie drones, open relays, and proxies. The result is that laws regulating commercial message content or form often constrain legitimate businesses but are ignored by illegal or fringe operators.

Authentication seeks to allow a recipient to verify who sent a message. Authenticated e-mail offers several benefits. First, the recipient can decide, either manually or automatically, to accept the message based on the actual sender's identity. Much SPAM is currently "spoofed" by listing a false or non-existent sender. Having authenticated sender information allows filters and whitelists to operate more efficiently and accurately, and makes evading blacklists of known violators more difficult. Authentication also makes enforcement easier and cheaper. If senders cannot hide their identities, law enforcement need not expend significant resources tracking down and proving who violators are. Finally, authentication may deter SPAMmers from violations since they can expect their identities to be revealed.

Cryptographic solutions to combat SPAM also appear promising. Yahoo!'s DomainKeys proposal, Cisco's Identified Internet Mail (IIM) method, and Bounce Address Tag Validation (BATV) all attempt to prevent falsification of sender's addresses by requiring a message's originator to encrypt at least part of the message with a private cryptographic key known only to the legitimate holder of the sender's address or domain. The recipient then uses a publicly-available cryptographic key (provided by the holder of the domain or address claimed as the sender) to decrypt the message. If the message can be decrypted, it originated with someone with access to the private key. Thus, the recipient can treat the message as legitimate.

These methods generally propose to distribute the public key information necessary to decrypt a received message through the Domain Name Server (DNS) system currently used to map domain names to Internet Protocol (IP) addresses. The proposals simplify implementation by allowing individual domain owners to manage their cryptographic keys, avoiding the need for a single overarching key authority. The current DNS system can store and retrieve cryptographic keys with no modification. However, each end-to-end scheme requires significant changes to both e-mail clients sending messages and the servers attempting to authenticate them. Since there are over thirty million Internet domains, any change to how e-mail works will certainly be adopted gradually, and many servers may never upgrade. Therefore, any authentication scheme will have to deal indefinitely with a significant volume of legitimate e-mail, which does not support authentication.

Microsoft and developer Meng Wong independently proposed authentication solutions that authenticate only the most recent connection that transferred a message, rather than authenticating the entire chain of transfer from the message's originator to the recipient. These proposals have been merged into a single proposal, "Sender ID for E-mail." Sender ID only authenticates the domain of the most recent message transferor; unlike end-to-end solutions, it cannot be extended to individual senders.

The primary advantage to last-hop solutions is that they do not require modification of the sender's mail server. Thus, domains can be made compatible with Sender ID even if their mail server cannot be modified. A domain can implement Sender ID for its outgoing messages with little time or effort by adding a new Sender Policy Framework (SPF) record to its DNS entry. Although Sender ID does not require modification of the sending server, the receiving mail server, or the recipient's mail client, must be modified to support Sender ID to authenticate the message. Thus, a last-hop solution provides an immediate method of supplying authentication information for messages that can be easily adopted by every sender. Only recipients who want to verify senders' information need modify their existing e-mail software.

Since enforcement of SPAM regulations requires identifying violators, legal systems have an interest in encouraging or mandating authentication. For example, the Federal Trade Commission, the agency responsible for enforcing the federal U.S. anti-SPAM act, has indicated that it may mandate an authentication protocol if market forces fail to supply a consensus choice. However, unless all systems adopt a compatible method, authentication is unlikely to simplify the difficult task of cross-jurisdictional enforcement. In addition, the economic costs and physical impossibility of universal adoption limit the extent to which states can mandate, rather than encourage, authentication. ITU believes it is worthwhile for states to discuss authentication technologies to increase the probability that a single technology, amenable to the varying needs of different systems, will be adopted.

Neither last-hop nor end-to-end authentication can distinguish legitimate messages from illegal messages sent by hijacked computers. If an authentication scheme is adopted that makes it impossible for messages to be sent anonymously, violators will increase efforts to compromise and use others' equipment to send their messages. States may need to create liability for third parties who do not take reasonable steps to prevent their equipment for being used for illegal purposes. For example, an ISP who failed to secure a mail server could be held liable if that server were used to send SPAM. In addition, universal adoption of any authentication method is unlikely given the large number of mail servers worldwide. This may make mandated authentication impossible; thus, legal regimes may instead move to provide incentives to entities, such as service providers, who voluntarily adopt solutions that make identifying violators easier.

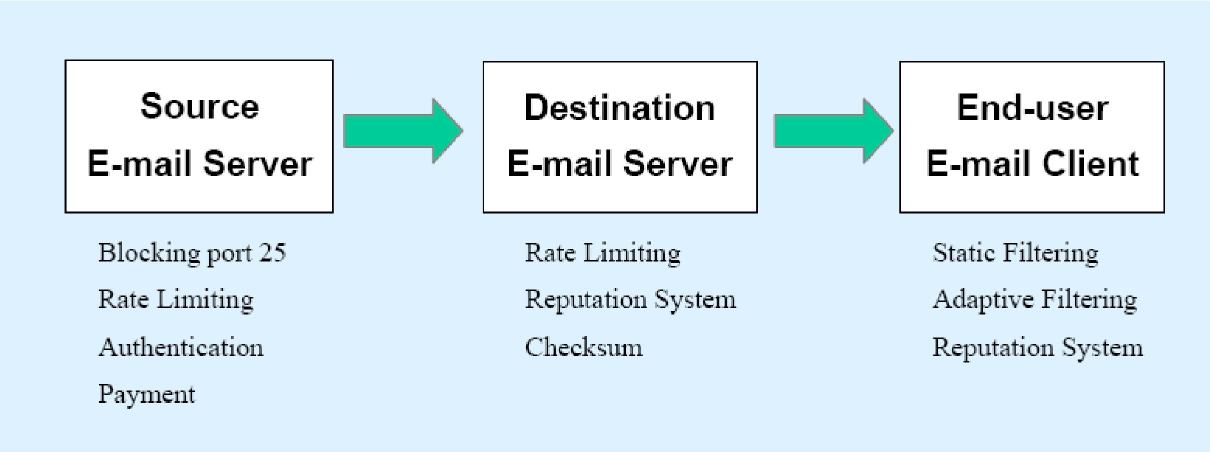
## Security

SPAM is intimately linked to computer and network security. Increasingly, SPAMmers use a distributed mechanism to transmit messages from multiple sources. This method involves compromising the security of numerous computers with high-speed Internet access through viruses or worms that exploit flaws in operating systems or a user's failure to install and maintain firewall and anti-virus software. Once compromised, these "zombie" computers send messages on behalf of the SPAMmer. This disguises the sender, evades ISP limits on the number of messages one source can transmit, and reduces the SPAMmer's hardware and bandwidth costs. Computer security company Symantec estimates that thirty thousand computers become zombies each day. Groups of these zombie computers, known as "botnets," are sold or rented for malicious purposes ranging from denial of service attacks to mass transmissions of SPAM. Thus, maintaining proper security – even for home computers – is vital to the success of efforts against SPAM.

Intermediaries such as ISPs and messaging service providers can, and do, take measures to improve security and to decrease the vulnerability of users and of networks. For example, Google's Gmail free e-mail service removes hyperlinks from messages that the service believes to be "phishing" attempts. ISP Earthlink requires all e-mail messages to route through its mail servers to reduce the impact of zombie networks and mandates that users' e-mail programs submit passwords to transmit messages. While these methods can reduce the burden of SPAM, it is important to recognize that end users must also exercise significant responsibility for maintaining a secure, safe computing environment. Users who do not update virus software and operating systems automatically or regularly, or who download programs that contain "malware" and "spyware" that compromise their computer, pose a risk not only to themselves but to other users worldwide. Thus, security measures must operate in conjunction with user education campaigns.

### ITU: Email Technical Solutions Overview

There are three different stages in the e-mail system where we can implement technical measures to curb SPAM: at the source where the e-mail is being sent out, at the destination where the e-mail is received, and finally at the end-user's e-mail client itself. The Figure below provides an overview of the various technical measures available at each stage.



### Source Email Server

At the source email server there are four technical measures to curb SPAM, they are listed as follows:

**1 Blocking Port 25**

To prevent users from sending outgoing mail via any third-party mail-hosting services it is advices to block Port 25.

It has been estimated that over 40 per cent of all SPAM is being sent out through zombie machines.9 Blocking port 25 will compel the sender to route his e-mail via his ISP's mail server. Such e-mail is then subject to the other anti-SPAM measures implemented by the sender's ISP (e.g. rate limiting). Blocking port 25 can be an effective SPAM countermeasure. Some ISPs implement the port 25 blocking selectively, for example, just on addresses that appear to be sending out large quantities of SPAM, other ISPs have gone as far as to adopt the tactic for all customers.

There is a disadvantage when blocking port 25; blocking port 25 can create problems by blocking legitimate e-mail as well as SPAM. There are some users who need to run their own mail server or communicate with a mail server on a remote network to submit e-mail (such as a web hosting company). ISPs should identify and not block port 25 for such customers.

One solution might be to require new subscribers to check a box in the service application indicating that they wish port 25 to remain unblocked. This will result in a default block of port 25 for the vast majority of home users who have never heard of and have no particular use for port 25. Such a selective approach can significantly cut down on SPAM entering our networks without stopping legitimate uses of port 25. Imposing rate limits on e-mail usage is already a fairly common practice among Internet Service Providers or ISPs as a way to stop bulk messages from leaving their e-mail server.

### 2 Rate Limiting

Rate Limiting – is to set a control on how many e-mails can be sent from the source e-mail server within a given timeframe.

By setting a limit that is high enough not to unduly restrict usage by legitimate users yet low enough to curb the activities of SPAMmers, it is possible to cut down on SPAM originating from the source e-mail server by a significant amount. The rate limiting measure is very attractive because most e-mail server software today can already be configured to implement this solution.

### 3 Authentication

Authentication is to provide a mechanism for the destination e-mail server or end-user's e-mail client to verify that the e-mail is indeed sent out by the source e-mail server. One significant weakness is that it currently allows any e-mail client to assert any identity—you can be whoever you claim to be.

The following is an illustration of how such authentication mechanism is used to prevent forgery:

- When the destination e-mail server receives an e-mail coming from a certain IP address, the e-mail claims to be from a certain sender but we need a way to find out if this is genuine.
- The authentication system will tell us one of three things:
    A. The sender is good – the sender has previously announced that they do send mail from that IP address.
    B. The sender is bad – the purported sender has published a list of IP addresses they send mail from, and the incoming IP isn't one of them.
    C. The sender is unknown – there is insufficient information to decide one way or the other.

The source server Mail Authentication System cannot stop SPAM by itself, but is rather intended to complement other anti-SPAM systems. Technically, it makes approaches such as domain-name blacklists and fine-grained reputation systems viable. Legally, it makes it easier to identify and take enforcement action against SPAMmers (e.g. for use of false header information).

### 4 Payment

Payment approach - is to provide a mechanism to charge the user for sending out e-mail via the source e-mail server. Such payment could be of monetary value or just computational resource cycles.

Perhaps, the ultimate end-all solution to SPAM is to start charging for every e-mail[26]. As with the rate limiting solution, the price to send each e-mail should be low enough to be affordable to an average e-mail user, yet high enough to make it prohibitively expensive for SPAMmers to send millions of e-mails a day. The monetary approach, known as "sender pays," has different variations and is currently being explored by several anti-SPAM companies. One company that advocates such an approach is a Silicon Valley start-up called Goodmail. Understandably, ISPs are interested in exploring this idea as it helps them defray the soaring costs of handling e-mail.

## Destination E-mail Server

At the destination email Server there are three technical measures to curb SPAM, they are listed as follows:

- Rate Limiting;
- Reputation System; and
- Checksum.

This is the most difficult place to implement any technical measures. As one person's junk e-mail is a source of useful information to another, it can be extremely challenging to implement any filtering mechanism at the destination e-mail server that can satisfy the majority of its users. Implementing some anti-SPAM measures at the destination server will prove to be beneficial because:

- End-user's mailbox storage space is limited[27] and the email inbox gets flooded with SPAM.
- End-user's bandwidth is limited (and costly to some users). Although end users can implement aggressive anti-SPAM measures on their desktop, they will still need to spend the time and bandwidth to download all the e-mails to their desktop to process them for SPAM.

### 1 Rate Limiting

Conceptually, it provides to set a control on how many e-mails can be received by the destination e-mail server within a given timeframe.

As with rate limiting at the source e-mail server, throttling the amount of e-mails that can be received by the destination e-mail server within a given timeframe is a simple yet effective solution against SPAM.

### 2 Reputation System

Conceptually, it provides a mechanism for destination e-mail server to determine if it should receive the incoming e-mail based on the known reputation of the source e-mail server.

[26] Considering at the same time the drawbacks mentioned before such as the increase in cost would prove crippling to many developing nations that are in the early stages of adopting new information and communications technologies infrastructures and the major changes required to the existing electronic mail infrastructure.

[27] Even with the wide spread of terabyte storage hardware; typically, there is an email inbox quota which defines a storage limit.

The reputation system is perhaps the most controversial anti-SPAM approach on the server-end. Essentially, it is a system where the destination e-mail server decides what is SPAM and what is not based on the known past reputation of the source e-mail server.

### 3 Checksum

Conceptually, it provides a mechanism for the destination e-mail server to determine if an incoming e-mail is of bulk nature (i.e. SPAM) by comparing the incoming e-mail against all the e-mails previously received by the destination e-mail server. An e-mail that is sent to a large number of recipients has a high likelihood of being SPAM.

An e-mail server receives lots of different e-mails everyday. It is usually difficult for the server (or even the server admin) to determine if a particular incoming e-mail is a SPAM or a non-SPAM, because every e-mail user has his own e-mail preferences and SPAM tolerance level.

## End-User E-mail Client

At the End User E-mail Client there are three technical measures to curb SPAM, they are listed as follows:

- Static Filtering;
- Adaptive Filtering; and
- Reputation System.

End-user side solutions can be far more aggressive because users exercise a very high degree of control over their incoming e-mails and because any action taken by users to tackle SPAM will affect only their own individual mailboxes.

By combining all these approaches in an end-user e-mail client, it is possible to achieve astonishing results in SPAM reduction on the end-user desktop mailbox.

### 1 Static Filtering Approach

Conceptually, it provides a mechanism through the end-user's e-mail client to screen incoming e-mails by comparing the various attributes of the incoming e-mail, for example, scanning the body of the e-mail to search for the word "sex".

The static filtering approach is the most fundamental anti-SPAM mechanism. It has been incorporated in most modern e-mail clients and services.

### 2 Adaptive filtering approach

Conceptually, it provides a mechanism through the end-user's e-mail client to screen incoming e-mails using a statistical approach. The end-user will need to train the system so that it can learn to adapt in the e-mail screening process.

The major shortfall with static filtering approaches is that it is difficult to be exhaustive in the generation of filtering rules.

### 3 Reputation system (end-user client)

Conceptually, it provide a mechanism through the end-user's e-mail client to determine if it should receive the incoming e-mail based on the known reputation of the sender.

To reduce false positives in SPAM classification using a filtering approach, the easiest way is to complement it with a reputation system.

### 4.4.3 MAAWG[28] AND APWG[29]

#### MAAWG Best Practices for Internet Service Providers and Network Operators

#### Best practices Context/Definitions:

In any given national jurisdiction, each of the Best Practices is understood to be recommended only if it is not in contradiction with existing national legislation. In the context of these Best Practices, ISPs and network operators include any entity operating a SMTP server connected to the Internet.

#### BIAC recommends to ISPs and Network Operators that:

1. Within the boundaries of the appropriate legal framework, ISPs and network operators address the problem of compromised end-user equipment by establishing timely processes to allow such end user equipment and network elements to be managed and eliminated as sources of SPAM;
2. ISPs and network operators utilize industry standard technology to authenticate their email and/or their sources;
3. ISPs and network operators block potentially infected email file attachments. In the case of filtering email or email file attachments based on content properties, in the context of any required legislation prior agreement is to be obtained from the customer;
4. ISPs and network operators actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and respond appropriately;
5. ISPs and network operators establish appropriate inter-company processes for reacting to other network operators' incident reports, also accepting end user complaints.
6. ISPs, network operators and enterprise email providers communicate their security policies and procedures to their subscribers;
7. ISPs and network operators attempt to send non-delivery notices (NDNs) only for messages originated by their own account holders;
8. ISPs and network operators take measures to ensure that only their account holders use their email submit servers;
9. ISPs and network operators ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information, and that this information includes points of contact for

[28] *Source: Messaging Anti-Abuse Working Group (MAAWG). On (www.maawg.org/)*

[29] *Source: The Anti-Phishing Working Group (APWG). On (www.antiphishing.org/)*

roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address;

10. ISPs and network operators ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries; that all local area network (LAN) operators are compliant with Request for Comments (RFCs) 1918 . "Address Allocation for Private Internets," and that in particular, LANs do not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.

## Anti-Phishing Best Practices for ISPs and Mailbox Providers

APWG and MAAWG have worked together to produce Anti-Phishing Best Practices for ISPs and Mail Box Providers, these best practices are shown in a document called “MAAWG Anti-Phishing Best Practices”. This section of the document has been divided in two sections, anti-phishing techniques and Anti-Phishing Best practices:

### A) Anti Phishing Techniques:

- Inbound Filtration of Protection Message.
- Outbound Protection schemes.
- Web Travel Filtration.

### Inbound Filtration of Phishing Messages

Inbound filtration of fishing messages has seven different techniques to combat SPAM, they are listed as follows:

- Filtration of Phishing Messages.
- Policy Considerations.
- End Point or client side Filtration.
- Forgery Detection with Sender Authentication.
- Conceal Images from Un-trusted Sources.
- Disable Hyperlinks from Un-trusted Sources.
- Visual Signals on Message Legitimacy.

The following are description of these techniques:

#### 1 Filtration of Phishing Messages

The most common front-line defense against phishing e-mails is the use of anti-phishing/anti-SPAM filtration technology at the outermost border Mail Transport Agent (MTA) or e-mail server. This is usually done using the same anti-SPAM software that the ISP already has in place to detect and filter SPAM.

The following are techniques that have been developed, and currently they are in use in order to filter SPAM:

- Bayesian content filters.
- IP address blacklists.
- Heuristics and Fingerprinting schemes.

- URL-Based Filters.

While all of these techniques are effective to varying degrees against SPAM, only some perform well against phishing.

A. Bayesian Filters

Bayesian classifiers filter SPAM based on their semantic difference from legitimate communications. Bayesian filters are in wide use, particularly in end-user anti-SPAM products. Most of the Bayesian filters in use today have been trained to detect SPAM. As such, it is rather difficult to detect phishing messages using Bayesian classifiers trained to detect SPAM. However, a Bayesian classifier specifically trained to detect phishing messages may do better. ISPs that deploy Bayesian filters should carefully measure the effectiveness of their filters against phishing messages.

B. IP Address Blacklists

IP address-based (source-based) filters created to detect SPAM are particularly poor at detecting phishing messages because phishing messages often originate from otherwise “good” hosts. As with Bayesian filters, ISPs should carefully evaluate the efficacy of their source-based blacklist solutions for recognizing and filtering phishing messages.

C. Heuristics and Fingerprint Schemes

A rules-based problem-solving technique. Heuristic-based, anti-SPAM and anti-phishing filters look for telltale signs in e-mail messages that indicate the message is SPAM or phishing. Heuristic solutions look for specific techniques used by phishers, such as encoding the name of a financial institution in the local part of a URL and using IP addresses as the host part of the URL. Fingerprinting schemes work by comparing known samples of phishing messages against incoming e-mail.

D. URL-based Filters

Some URL-based filters look for specific IP addresses, domains, or URLs where known phishing web pages are hosted. URL-based filters are fairly effective, but based as they are on limited reporting, can represent only a small sample of phishing activity at any given moment.

Further, it MAAWG and APWG state that ISPs should conduct comprehensive field trials specifically targeted at phishing security before deploying an anti-phishing filtration solution. Ideally, ISPs should compare multiple solutions to determine their efficacy at stopping phishing attacks.

## 2 Policy Considerations

In many messaging security systems, SPAM is often marked, but then delivered to either a user’s inbox or to a special “SPAM” folder, which allows users to review a message and personally determine whether it is SPAM or legitimate e-mail. With phishing messages, rather than delivering a distinguished phishing message to users, it is advised that the ISP reduce the message or reject it at the SMTP level. Because phishing messages are designed to impersonate legitimate messages, many users cannot accurately assess the message as a phishing attempt. Additionally, it is recommended that:

- Deny/reject phishing messages where possible.
- When it is not possible to drop messages (due to user request, ISP policy, or legislative requirements), ISPs should indicate to the user that they are phishing messages and although they might look legitimate, they are dangerous and should be ignored.

### 3 End Point or client side Filtration

There are several free and commercial end-point security solutions on the market that plug in to users' e-mail software and filter phishing messages from incoming mail. In instances where an ISP is unable to provide server-level phishing filtration, these solutions can be effective. End-point solutions are also recommended so that users can be protected when they are accessing e-mail from multiple accounts, some of which may not reside on the ISP infrastructure. MAAWG and APWG say that ISPs should encourage their users to employ end-point security solutions to combat phishing.

### 4 Forgery Detection with Sender Authentication

E-mail authentication is becoming widely adopted. Among other things, e-mail authentication can be used to determine if the sender has forged the sender identity. Phishers often try to forge the information in the headers to make it appear as if the message originated from a legitimate institution. Sender authentication, where available, can often be used to detect this. Moreover, MAAWG and APWG states that ISPs should filter or reject e-mail if they can unequivocally determine that the Sender's identity is forged.

### 5 Conceal Images from Un-trusted Sources

E-mail providers long ago disabled JavaScript® and other executables for all incoming e-mail messages. There is now a positive trend to disable images by default, and to display images only when embedded in trusted messages.

Further, it is recommended by MAAWG and APWG that ISPs should consider turning off images for all messages for which the identity and reputation of the sender cannot be established, and provide the user the ability to enable those images.

### 6 Disable Hyperlinks from Un-trusted Sources

Another method of improving the threat of phishing is to halt hyperlinks in un-trusted e-mail. This makes it more difficult for phishers to trick users into clicking through to a fraudulent site. ISPs should disable all hyperlinks in e-mail from un-trusted sources. ISPs also should remove hyperlinks from suspected phishing e-mails. ISPs are recommended also to consider turning off images for all messages for which the identity and reputation of the sender cannot be established, and provide the user the ability to enable those images.

### 7 Visual Signals on Message Legitimacy

In parallel with their continued effort to block phishing messages, some mailbox providers also support a mechanism that conveys the authenticity of legitimate messages to their users within their e-mail interface. Although it has been suggested to allow senders to include images inside of the message itself, those images are easily faked. Instead, our recommendation is that these visual cues should appear in an area of the user interface (UI) that cannot be altered or spoofed. This may require changes to the e-mail client or web-based e-mail interface.

Recommendations:

- ISPs should consider providing their users visual cues (an icon in the message list view and/or in the message view) highlighting messages known to be legitimate and from trusted sources.
- Each ISP should determine to what level they are comfortable endorsing presumed or known to be legitimate messages, and convey this endorsement level to users. The endorsement level depends on the ISPs' confidence in the underlying vetting technology and processes.
- This recommendation applies to situations in which the ISP controls the user interface (webmail, proprietary MUA, plug-in for off-the-shelf MUA).

### Outbound Protection Scheme

Phishers often launch their attacks from compromised servers, without the knowledge of the owner of the server or the surrounding network. Often, these unsuspecting carriers are end-user machines connected to an ISP via dial-up, DSL or cable modem.

ISPs should consider outbound content filters. When considering an inbound filter, ISPs should also evaluate the outbound capabilities of the solution.

General Recommendations for the ISPs:

- ISPs should ensure that their DNS architecture is up-to-date. Old software or systems are more likely to be vulnerable to attacks, and can lead to the compromise of a DNS server, thus putting all users of that server at risk for pharming attacks[30].
- ISPs should remember that phishing and SPAM are not synonymous. Train your support representatives to recognize the difference.
- If a user reports suspicious e-mail asking for personal information, the ISP should inform the user of the dangers of phishing attacks, and warn him or her against giving out personal information online. The user should be further advised to send a copy of the e-mail to the ISP, so it can be used to update filters.
- If the user believes that he or she has been scammed, the user should be urged to file a complaint with the appropriate anti-fraud organization such as the Federal Trade Commission (FTC).
- Customer support processes should be in place for quick remediation in cases where a suspected phishing e-mail or site is sent from or hosted by the ISP itself.
- Customer support should also direct users to consumer education resources that enables them to understand the nature and scope of these threats, and which describe measures the ISP is taking to protect users.

[30] a cracker's attack aiming to redirect a website's traffic to another, bogus website.

### Web Travel Filtration

Phishing messages contain one or more links to a phishing website to collect user credentials. One way to render phishing attacks useless is to block access to these sites. There are several free and commercial efforts underway that provide lists of known phishing URLs to organizations that wish to limit access to these URLs. ISPs should enable short-lived blocks on confirmed phishing sites using firewalls and/or web-filtration products.

Recommendations:

- Where possible, ISPs should enable short-lived blocks on confirmed phishing sites using firewalls and/or web-filtration products.
- ISPs should bundle, distribute, or encourage their users to download web browser plugins that detect and restrict access to known or suspected phishing sites based on phishing URL feeds and/or predictive heuristic technologies. Certain plug-ins also authenticates legitimate websites and instill confidence in users about the safety of their web experience.

## B) Anti Phishing Best Practices:

- Email Transmission.
- Benefits of Adoption.
- ISPs to Phishing Target Communications.

### Email Transmission

Industry self-regulation is the most effective measure to address email transmission abuse, and the magnitude of the SPAM problem demands immediate action. The message has been received loud and clear from government agencies worldwide: absent immediate action and results, the industry faces increased scrutiny and regulation. Therefore, the MAAWG recommends the following set of Email Transmission Best Practices for Internet and Email Service Providers, ESPs/ISPs:

- Should Provide Email Submission services on port 587[31].
- Should require authentication for Email Submission.
- Should abstain from interfering with outbound connectivity to port 587.
- Should configure email client software to use port 587 and authentication for Email Submission.
- Should block access to port 25 from all hosts on their network, other than those that you explicitly authorize to perform SMTP relay functions. Such hosts will certainly include your own Email Submission servers and may also include the legitimate Email Submission servers of your responsible customers.

[31] According to the Request for Comments: 2476, Message Submission, found at: http://www.rfc-editor.org: Port 587 is reserved for email message submission. Messages received on this port are defined to be submissions. The protocol used is ESMTP [SMTP-MTA, ESMTP], with additional restrictions as specified here. While most email clients and servers can be configured to use port 587 instead of 25, there are cases where this is not possible or convenient.

- Should block incoming traffic to their network from port 25. This prevents potential abuse from SPAMmers using asymmetric routing and spoofing IP addresses on their network.
- These practices have been adopted by providers of all sizes, including many of the most popular service providers in the world and many MAAWG members, without any appreciable reduction in customer base.

## Benefits of Adoption

Requiring authentication and aggregating email transmission traffic through SMTP relays provides an ISP with many valuable benefits. These measures enable the ISP to:

- Identify the party responsible for submitted messages.
- Filter out SPAM, viruses, and other abusive message payloads.
- Monitor and limit, per customer and/or in aggregate, transmission rates.
- Enforce acceptable use policies and terms of service for email submission.
- Additionally, the ISP gains the following competitive advantages:
- Improved deliverability for legitimate email messages, because of a reduced risk of being blacklisted by receiving Internet and Email Service Providers.
- Reduced costs for abuse help desk, customer support, and network operations centres.
- Ability to offer premium tiers of service to customers who have a legitimate need to operate email servers with direct access to port 25.
- Reduced infrastructure costs due to reductions in port utilization and bandwidth consumption.
- Proportionate recipient's share in the global reduction of SPAM volumes.

Once these measures are in place, infected machines can no longer be vehicles of anonymity. Victimized computers can be rapidly identified and quarantined until the owner becomes aware of the problem and corrects it. In the process, customers are educated about security threats and are encouraged to better protect themselves. Each of these changes increases the safety and privacy for all end users.

## ISP-to-Phishing Target Communications

ISPs should try to communicate early knowledge of phishing attacks to the targeted institution. ISPs should communicate knowledge of phishing attacks to the targeted institution via the Anti-Phishing Working Group at www.antiphishing.org, or via a similar, regional organization.

### 4.4.4 SPAMHAUS[32]

The SPAMhaus Project is a completely volunteer effort that aims to track e-mail SPAMmers and SPAM-related activity.

SPAMhaus publishes the Register Of Known Spam Operations (ROKSO) - a database collating information and evidence on the '200' known worst SPAM gangs worldwide, used by ISPs to avoid signing up known spammers who would abuse their networks and by Law Enforcement Agencies to help target and mount prosecutions against professional SPAMmers.

SPAMhaus publishes a number of real-time SPAM-blocking databases, including the SPAMhaus Block List (SBL), the Exploits Block List (XBL) and the Policy Block List (PBL). Broadcast from a network of 40 DNS servers in 17 countries, the SPAMhaus blocklists are used by many of the Internet's major Internet Service Providers, Corporations, Universities, Governments and Military networks.

Many internet service providers and other Internet sites use these free services to reduce the amount of SPAM[33]. The SBL, XBL and PBL collectively protect over 500 million e-mail users, according to SPAMhaus' web page (December 2006). Like most DNSBLs, their use is controversial. The following are the explanation of different types DNSBLs:

#### The SPAMhaus Block List (SBL)

The SPAMhaus Block List ("SBL") Advisory is a database of IP addresses which do not meet SPAMhaus's policy for acceptance of inbound email and therefore from which SPAMhaus does not recommend the acceptance of electronic mail. IP addresses are listed on the SBL because they appear to SPAMhaus to be under the control of, or made available for the use of, senders of Unsolicited Bulk Email ("SPAMmers"). The SBL database will normally include IPs identified to SPAMhaus's best ability as direct SPAM sources, SPAMmer hosting/DNS, SPAM gangs and SPAM support services.

SBL listings are based on SPAMhaus' definition of "SPAM" meaning "Unsolicited Bulk Email" ("UBE"). SPAMhaus does not evaluate the content or legality of SPAM, merely whether a message is SPAM by our definition or not. The responsibility for complying with SPAMhaus SBL policy and preventing UBE being sent begins and ends with the bulk email sender.

SBL listings are backed up with evidence which has fully satisfied the SBL team that the IP address or IP range is under the control of a SPAMmer, SPAM operation or a SPAM support service and represents an unwanted nuisance or threat to mail systems using the SBL.

SBL listings are immediate and, in the case of known SPAM gangs, are preemptive. The SBL does not require warnings or have a 'grace period' and does not require physical evidence of SPAM received from any specific IP to qualify a listing (in the case of known SPAM gangs, any IPs under their control are listed on sight). Warnings are however normally sent to block owners and/or Upstreams before listing large netblocks.

[32] *Source: PAMHAUS. On (www.SPAMhaus.org/).* To know about the latest worst Spammers/Networks/Countries, please check the SPAMHAUS. SPAMHAUS offers two types of services: paid Data Feed service only to qualified organizations (ISPs, companies, universities, government networks) (for ISPs, Governments, Military agencies and companies) and free services for individuals and small companies.

[33] In fact there are free and paid services in this regard. For instance, 'MAPS Relay Spam Stopper' available at http://work-rss.mail-abuse.org/rss/index.htmloffers paid services while 'Arbitrary black hole list' available at http://abl.v6net.org/ offer black lists for free.

### Listing Criteria

The criteria for listing IP addresses in the SBL are:

| | |
|---|---|
| SPAM Sources | Sources of unsolicited bulk email sent to SPAMhaus SPAMtraps or submitted to SPAMhaus by trusted 3rd party intelligence. |
| SPAM Services | Servers, including mail, web, dns and other servers identified as being an integral part of a SPAM operation or being under the direct control of SPAMmers. |
| SPAM Operations | Known SPAM operations and gangs listed in SPAMhaus ROKSO registry, including preemptively listing new IPs each time known SPAMmers move to new hosts. |
| SPAM Support Services | Services providing service to known SPAM operations listed on ROKSO, services providing 'bullet-proof hosting' for SPAM service purposes, services obfuscating or anonymising SPAM senders, services selling or providing hosting for the sales or distribution of SPAMware or address lists, and networks knowingly hosting SPAMmers as either stated or de facto policy. |

### Notifications of Listings

SPAMhaus maintains a database of worldwide Internet Service Providers which includes the ISP's contact address for abuse issues (where known). On creating a new SBL record the SBL database automatically emails a notification of the listing to the ISP's abuse contact (where known).

### Delisting

IP addresses are removed immediately from the SBL database upon receipt by the SBL Team of notification from the IP owner (the Internet Service Provider responsible for assigning or routing the IP address) that the reason for listing has been corrected or terminated.

### Updating

SPAMhaus does not perform scans to update SBL records. It is the ISP's responsibility to advise the SPAMhaus Project of any changes which affect a listing. On being advised of changes, SPAMhaus will endeavor to amend the listing as quickly as possible.

### Timeouts

If not removed manually from the database, all SBL records eventually time out and are automatically removed. Each SBL record has a timeout value set by the record Editor as deemed appropriate for the listing. Unidentified SPAM sources normally have a short time-out of 2, 7 or 14 days, persistent SPAMmers may have a timeout set at 6 months, while known SPAM gangs with ARIN-assigned IPs will normally have the timeout set at one year or more.

### SPAMhaus Don't Route Or Peer (DROP)

DROP (Don't Route Or Peer) is an advisory "drop all traffic" list, consisting of stolen 'zombie' netblocks and netblocks controlled entirely by professional SPAMmers. DROP is a tiny sub-set of the SBL designed for use by firewalls and routing equipment.

DROP is currently available as a simple text list, but will also be available shortly as BGP with routes of listed IPs announced via an AS# allowing networks to then null those routes as being IPs that they do not wish to route traffic for.

The DROP list will NEVER include any IP space "owned" by any legitimate network and reassigned - even if reassigned to the "SPAMmers from hell". It will ONLY include IP space totally controlled by SPAMmers or 100% SPAM hosting operations. These are "direct allocations" from ARIN, RIPE, APNIC, LACNIC, and others to known SPAMmers, and the troubling run of "hijacked zombie" IP blocks that have been snatched away from their original owners (which in most cases are long dead corporations) and are now controlled by SPAMmers or netblock thieves who resell the space to SPAMmers.
When implemented at a network or ISP's 'core routers', DROP will protect all the network's users from SPAMming, scanning, harvesting and dDoS attacks originating on rogue netblocks.

SPAMhaus strongly encourages the use of DROP by tier-1s and backbones.

## The Exploits Block List (XBL)

The SPAMhaus Exploits Block List (XBL) is a realtime database of IP addresses of illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, wingate, etc), worms/viruses with built-in SPAM engines, and other types of trojan-horse exploits.

### Incorporates CBL data and NJABL proxy data

The XBL wholly incorporates data from two highly-trusted DNSBL sources, with tweaks by SPAMhaus to maximize the data efficiency and lower False Positives. The main components are:

- The CBL (Composite Block List) from cbl.abuseat.org; and
- The NJABL Open Proxy IPs list from www.njabl.org.

Mail servers already using cbl.abuseat.org should NOT also use xbl.SPAMhaus.org or you will be making 'double' queries to basically the same data source and only one DNSBL will appear to work (the other(s) will appear to not catch anything). Mail servers already using dnsbl.njabl.org are advised to continue doing so, as dnsbl.njabl.org is itself a composite list and contains more than the open proxy IPs list part now incorporated in XBL.

## The Policy Block List (PBL)

The SPAMhaus PBL is a DNSBL database of end-user IP address ranges which should not be delivering unauthenticated SMTP email to any Internet mail server except those provided for specifically by an ISP for that customer's use. The PBL helps networks enforce their Acceptable Use Policy for dynamic and non-MTA customer IP ranges.

PBL IP address ranges are added and maintained by each network participating in the PBL project, working in conjunction with the SPAMhaus PBL team, to help apply their outbound email policies.

Additional IP address ranges are added and maintained by the SPAMhaus PBL Team, particularly for networks which are not participating themselves (either because the ISP/block owner does not know about, is proving difficult to contact, or because of language difficulties), and where SPAM received from those ranges, rDNS and server patterns are consistent with end-user IP space which typically contain high concentrations of "botnet zombies", a major source of SPAM. Once aware of them, the ISP/block owner can take over such records at any time to manage them further.

The PBL lists both dynamic and static IPs, any IP which by policy (whether the block owner's or -interim in its absence- SPAMhaus' policy) should not be sending email directly to the MX servers of third parties.

#### IP Address Self-Service Removal Mechanism

A feature of the PBL is the elimination of 'false positives' with a server-identifying and automatic removal mechanism for single IP addresses. This allows end users with static IP addresses within a larger dynamic pool, and legitimate mail server operators, to assert that in their opinion their IP addresses are a trustworthy source of email and to automatically remove (suppress) their IP addresses from the PBL database. Safeguards are built in to prevent abuse of this facility by SPAMmers (and particularly by automated bots).

#### Registry of Known SPAM Operations (ROKSO)

The Register of Known SPAM Operations (ROKSO) is a register of known professional SPAM operations ("SPAM gangs") that have been thrown off Internet Service Providers 3 times or more and are therefore repeat offenders. SPAMhaus believes that these known and determined SPAMmers are responsible for approximately 80% of SPAM on the Internet.

The ROKSO database collates information and evidence on each gang to assist ISP Abuse Desks and Law Enforcement Agencies.

The existence of these known professional SPAMmers, the aliases they use to obtain ISP accounts, their methods and history is vital need-to-know information for the ISP industry.

### 4.4.5 INTERNET ENGINEERING TASK FORCE (IETF)[34]

The Internet Engineering Task Force (ITEF) includes a large international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Request for Comments (RFCs) are the working notes of the Internet research and development community. These documents contain protocol and model descriptions, experimental results, and reviews.

[34] *Source: The Internet Engineering Task Force (IETF). On (www.ietf.org/).*

Few RFC-SPAM related were released by IETF such as:

- RFC4406: Sender ID: Authenticating E-Mail, April 2006

  This RFC describes a mechanism such that receiving Mail Transfer Agents (MTAs), Mail Delivery Agents (MDAs), and/or Mail User Agents (MUAs) can recognize mail in the above category and take appropriate action. For example, an MTA might refuse to accept a message, an MDA might discard a message rather than placing it into a mailbox, and an MUA might render that message in some distinctive fashion. The document defines a pair of closely-related tests. One validates a message's Purported Responsible Address (PRA). The other validates a message's Reverse-Path (also known as MAIL-FROM address). An e-mail sender complying with this specification should publish information for both tests, and should arrange that any mail that is sent will pass both tests. An e-mail receiver complying with this specification should perform at least one of these tests.

- RFC4405, SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message, April 2006

  The RFC proposes a specification in which the responsible submitter is the entity most recently responsible for injecting a message into the e-mail transport stream. The e-mail address of the responsible submitter will be referred to as the Purported Responsible Address (PRA) of the message.  The Purported Responsible Domain (PRD) is the domain portion of that address. This specification codifies rules for encoding the PRA into the Simple Mail Transfer Protocol (SMTP) transport protocol. This will permit receiving SMTP servers to efficiently validate whether or not the SMTP client is authorized to transmit mail on behalf of the responsible submitter's domain. This RFC describes a unified approach to combat SPAM. It uses the SMTP mechanism to describe an extension to the SMTP protocol. Using this extension, an SMTP client can specify the e-mail address of the entity most recently responsible for submitting the message to the SMTP client in a new SUBMITTER parameter of the SMTP MAIL command.  SMTP servers can use this information to validate that the SMTP client is authorized to transmit e-mail on behalf of the Internet domain contained in the SUBMITTER parameter.

- RFC3685, SIEVE Email Filtering: SPAMtest and VirusTest Extensions, February 2004

  This RFC introduces two SIEVE35 tests that can be used to implement 'generic' tests for SPAM and viruses in messages processed via SIEVE scripts.  These tests return a string containing a range of numeric values that indicate the severity of SPAM or viruses in a message, or a string that indicates the message has not passed through any SPAM or virus checking tools. The SPAM and virus checks themselves are handled by the underlying SIEVE implementation in whatever manner is appropriate, and the implementation maps the results of these checks into the numeric ranges defined by the new tests. Thus a SIEVE implementation can have a SPAM test that implicitly checks for third-party SPAM tool headers and determines how those map into the SPAM test numeric range.

[35] Sieve is a language for filtering e-mail messages. It is designed to be implemented on either a mail client or mail server. It is meant to be extensible, simple, and independent of access protocol, mail architecture, and operating system.

- RFC2635, DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (SPAM*), June 1999

This RFC provides guidelines concerning SPAM and covers three main areas. First, the RFC explains why mass unsolicited electronic mail messages are harmful in the Internetworking community. It shows that email SPAM has more burdens on the receiver than regular mails. It also emphasizes on the importance of fighting SPAM since an increase in the number of unwanted email (SPAM) can affect the email system as trusted communication medium. Second, the RFC gives a set of guidelines for dealing with unsolicited mail for users, system administrators, news administrators, and mailing list managers. It suggests that taking advantage of screening technologies can provide a mechanism to prevent SPAM. Users can install such technologies to their PCs to stop SPAM. System administrators and news administrators can use more intelligent screening software to detect SPAM in emails or posts. Firewalls can also be used in this regard. Finally, the RFC makes suggestions that Internet Service Providers (ISPs) might follow in order to reduce SPAM. For example, if the ISP doesn’t want to tolerate SPAM then it can write a clear Acceptable Use Policy (AUP) which states consequences for abuse. This policy should be set with downstream providers and the ISP should also be aware of their upstream providers’ policies. ISPs are also responsible for education their customers about SPAM and its dangers and what precautions they should take so that they don’t become senders or victims of SPAM.

- RFC2505, Anti-SPAM Recommendations for SMTP MTAs, February

This RFC gives a number of implementation recommendations for Simple Mail Transfer Protocol (SMTP), Mail Transfer Agents (MTAs) to make them more capable of reducing the impact of SPAM. The intent is that these recommendations will help clean up the SPAM situation, if applied on enough SMTP MTAs on the Internet, and that they should be used as guidelines for the various MTA vendors. The implementer should be aware of the increased risk of denial of service attacks that several of the proposed methods might lead to. A brief summary of this memo is:

  - Stop unauthorized mail relaying.
  - Spammers then have to operate in the open; deal with them.

- Design a mail system that can handle SPAM1999

## 4.5 EDUCATION AND AWARENESS INITIATIVES

### 4.5.1 OECD

OECD released various recommendations and suggestions regarding the anti-SPAM awareness and education. Generally, OECD recommends that SPAM awareness and education target:

- Student, Children, and Parents;
- Individuals;
- ISPs/ESPs; and
- Business Entities, especially SMEs.

Direct Marketers. Several players were targeted as described in the following:

- A comprehensive anti-SPAM strategy must ensure that the end-user, who is the final recipient of SPAM, the possible victim of viruses and scams, and, at the same time, the person who has control over their computer and personal information, is sufficiently educated and aware of how to deal with SPAM and other online threats. Education and awareness raising activities are needed in large enterprises, small and medium enterprises, for residential users and in education establishments. They must aim to create a culture of security, and encourage a responsible use of cyberspace".
- Consumer education and awareness, customer support, & online operators should communicate effectively with their customers. They should clarify which kind of communications can/will be sent by e-mail, define how e-mail addresses and other information may be accessed and modified by the user, specify that the user will never be asked to provide their personal data via e-mail, and list elements users need to verify in the message to be sure it is from the online operator.

**Direct Marketers should**

- Adopt and effectively implement a code of conduct using best practices for electronic marketing, which include marketing messages sent by e-mail, instant messaging, or mobile.

**Individual Users**

**Governments should:**

- Develop public information and awareness campaigns to educate end-users as to the products and services they are using and the associated risks they may face, thus allowing users to protect themselves from SPAM, viruses and other malicious codes. This information should be made available also on ISPs portals.
- Organise nation-wide campaigns to enhance media attention and of the population at large.
- Work with private sector, civil society and other interested parties on user education campaigns initiatives.

Given their ability to reach individual users on the web, ISPs and other network operators, including mobile operators, should use their company-customer communication channels (website, portals, SMS, newsletters) to provide information to their customers on:

- How to avoid SPAM and risks connected with SPAM e-mails, SMS, MMS, etc.
- Available anti-SPAM and anti-virus filter, open source solutions for the concerned platform.
- Indications on how to report SPAM abuses to the ISPs or the user's operator and to competent authorities, and
- E-mail/phone contact to the provider abuse desk.

### Users' groups:

- Computer classes for senior citizens, also financed by the government or local authorities, should include information on computer security, and practical examples on how to avoid SPAM, online frauds, viruses and other malicious software.
- Awareness on online threats and security issues should be part of students and children computer classes. Cartoons and comics could also be used to reach out to young users.

### Large Companies and SMEs:

- Companies: IT support should make available to new staff a pamphlet explaining the company's security policy for e-mail, existing filters and best practices for dealing with SPAM and how to avoid being SPAMmed. The same kind of information should be available on the internal website, and updates should be sent to users periodically.
- Small-medium-sized enterprises: Commercial associations, ISPs and security software companies should provide SMEs specific information on simplified security management practices, training material, free open source software, etc. Examples and resource materials are available on the OECD Task Force Website at www.oecd-antiSPAM.org.

The education of recipients is as important as the education of senders. Regulators and business associations can play an important role in educating companies by disseminating information on how business can communicate with their clients using electronic messaging, such as e-mail, in a manner that complies with national legislation.

Direct marketing associations should inform their members of relevant anti-SPAM legislation in force in their country of origin and in the country of destination of the message. Online marketing best practices and informational WebPages should be developed and co-ordinated at the international level.

### Industry cooperation and educational initiatives

- Co-operation among different organisations is a must in order to deliver a consistent, well-informed message to a target audience. Industry co-operation is one example. Different parties in an industry sector can develop a programme of self-regulation among members and may develop a programme which can be used to educate their customers on how to fight against SPAM.

- Internet Service Providers (ISPs) at the national level, and even at the international level, could develop codes of conduct to deal with SPAM. ISPs need to cover their clients who send outgoing e-mail in such codes of conduct. In this context the sharing, and adoption, of best-practice acceptable use policies by customers plays an important role.
- In addition, ISPs can play a role in educating their customers who are recipients of SPAM and teach them the basics of good Internet practice.
- Many Direct Marketing Associations across Europe, North America, and Australia have implemented Codes of Conduct for members to follow. These have been put into place to ensure that their members comply with marketing legislations and to prevent direct marketers from becoming SPAMmers unwittingly.

### 4.5.2 ITU

General Recommendations:

- As SPAM has become a societal problem, further attention should be paid to consumer education and awareness as an important step to decrease SPAM.
- Consumer education has been seen as a key element particularly important for the success of anti-SPAM legislation
- Increasing awareness of users of the risk of leaving e-mail addresses on numerous websites is a first step to prevent address harvesting. At the same time, that would make it harder and more costly for SPAMmers to obtain those addresses.
- The effects of consumer's awareness are not limited to SPAM coming from a particular country. If people are more careful about their email addresses that would also give them a certain protection against SPAMmers from third countries.
- Governments make sure that consumers are aware of where they can complain, what will be investigated, what action may be taken, and what information they need for authorities to launch an investigation.
- While it is important to act at the local level—by creating, for example, an appropriate legal anti-SPAM framework, building awareness, educating consumers and establishing dialogue and partnership with the private sector—any anti-SPAM measure should be considered at the international level.

## 4.6 SPAM MEASUREMENT

### 4.6.1 OECD

SPAM is evolving, although there are many different sources providing data on the amount of e-mail categorized as SPAM, the percentage of viruses and the number of phishing scams sent through electronic messages, the information is not easily comparable, and diverging results are reported. This is due to lack of a common international definition of SPAM, and to the different methodologies used to measure the amount of SPAM, which depend on the various filtering technologies employed.

Most of the data on SPAM originates from industry, in particular from anti-SPAM solution providers, but also by Internet Service Providers (although the latter data are not usually available to the public). Data gathered by these players are difficult to compare as they relate to a different user base and are founded on different parameters. This raises a number of questions about the completeness of data, what is being measured, and if industry should be encouraged to develop a single methodology for data collection. In addition, Internet Service Providers are often unwilling to disclose information which is sensitive for the company and may damage their competitiveness.

Filtering companies and ISPs (using filters) collect data from their customers that provide measures on the amount of SPAM detected by the filters. These data provide an indication of the growth of SPAM relative to the total volume of e mail, the different possible content, and the affected countries. Anti SPAM organizations and bodies related to consumer or privacy protection also measure SPAM. In addition, but to a limited extent, data on SPAM are collected by some governmental or public organizations which have the responsibility to develop anti SPAM policies or regulations.

Measurement is key to evaluating the evolution of SPAM and the effectiveness of anti-SPAM solutions and educational efforts, to be able to determine if a strategy is effective, and eventually what changes are needed in policy, regulatory and technical frameworks.

In order to better assess the current status of SPAM, and provide data on the amount of SPAM which passes in the network, the Messaging Anti-Abuse Working Group (MAAWG), in the context of the Task Force work, developed an E-mail Metrics Program and agreed on a series of ISPs SPAM indicators to measure:

- The total number of dropped connections resulting from IP blocking (while this parameter may be imprecise, it gives a sense of the magnitude of the amount of messages which are not penetrating the networks).
- The total number of blocked or tagged inbound e-mails and percentage of e-mails going through the ISPs (excluding blocked connections) that are identified as SPAM.
- The focus is therefore on “unwanted” e-mail, so that the difficulty of defining SPAM will be avoided.

ISPs’ data can be compared with measurements of SPAM as it is perceived by the user, in their inbox after the application of filters and other technical solutions. In order to obtain a more detailed analysis of the SPAM phenomenon, France undertook a statistical study based on «inbox SPAM». The preliminary results of the study, based on public statistical rules, suitably complete the existing statistical information. The idea was not to examine these e-mails one by one, but to study what kind of SPAM was being sent and which companies were the greatest offenders. 320000 messages were received during the 3-month duration of the program and five companies became subject to legal enquiries.

During the study, it was observed that most spam was aimed at individuals, since the contents are usually offers of products or services likely to interest them. Most SPAMmers were found to be small or medium sized companies looking for a cheap way to advertise their products.

Regarding the contents of the messages, notable differences appeared between those of the French language and those of the English language.

In the case of the English language spam, one can notice the important presence of SPAM in the financial sectors and health, respectively 40% and 12.9%. This proportion is not found within the French spam and can be explained by a stricter legislative framework and supporting laws in France and in the European Union unlike the United States.[36]

### 4.6.2 Messaging Anti-Abuse Working Group (MAAWG)

The Email Metrics Program developed by the Messaging Anti-Abuse Working Group (MAAWG) organizes compiled data into an unbiased tool for estimating the level of abusive messages in the email stream. This data is provided voluntarily and confidentially by Internet Service Providers, network operators and email providers that have come together in MAAWG to work against online abuse.

Participating members include Bell Canada, Comcast, Cox Communications, Microsoft Corp., Outblaze Ltd., TDC and TDS Telecom, among others. MAAWG members are under no obligation to supply this information or participate in the metrics reporting program. The data is shared at the discretion of each company and is reported here as aggregated metrics to support the industry’s efforts in preventing abuse from reaching individual user mailboxes. The MAAWG Email Metrics Program provides aggregated data covering almost 500 million mailboxes[37].

Statistics derived by MAAWG are based on the measurement of the following:

- **Number of Mailboxes Represented** - This is the total current customer mailbox count at the end of the quarter. This metric is reported in million of mailboxes.
- **Number of Dropped Connections and Blocked/Tagged Inbound Emails** – Taken together, dropped connections and blocked/tagged inbound emails are a measure of "abusive emails." The Number of Dropped Connections is the total connections dropped by using RBLs (Real Time Blacklists) and other devices. The Number of Blocked or Tagged Inbound Emails is the total number of emails blocked or tagged by a provider using commonly applied devices such as ASAV (Anti-SPAM/Anti-Viral) framework, MTAs (Mail Transfer Agents) and other recipient or message based rules. The sum of three months of dropped connections and blocked or tagged inbound emails is reported in billions. In this report, one dropped connection is equivalent to one blocked or tagged inbound email.

[36] For further information regarding the statistics results, please refer to the following web site: http://www.cnil.fr/

[37] Reports published by MAAWG can be found at http://www.maawg.org/about/EMR/. In its latest report, published in June 2007 covering the first quarter of 2007, MAAWG organised the data compiled over six quarters into this report. The report shows that about 75 percent of email traffic identified as abusive messaging (not SPAM, as SPAM definition is not defined in this report because, according to MAAWG, SPAM definition can vary from country to country and between jurisdictions as well). The report shows that the metrics continue to reflect the continuing high level of abusive email the industry works to prevent from clogging users’ inboxes and the need for continued industry cooperation and diligence.

- **Number of Unaltered Delivered Emails** - This is the total number of emails that were not blocked or tagged by the network operator’s anti-abuse efforts and were delivered to customers. The sum of three months of delivered emails is reported in billions.

## 4.7 INTERNATIONAL CO-OPERATION AND EXCHANGE

### 4.7.1 OECD

OECD recommends the following:

**National co-ordination should be first priority**

Multiple authorities have responsibility over investigation and/or enforcement of the various laws that can be violated by SPAMmers and do not, in most cases, co-ordinate to fully exploit synergies, means and resources. Some countries already have a co-ordination mechanism in place. For example, in Australia four agencies have an agreement to cooperate on SPAM-related matters. The United States has a central contact point to facilitate communication among agencies responsible for SPAM at federal and state level. Other countries also need to further efforts to strengthen domestic inter-agency co-operation and to designate one agency as a contact point for foreign authorities would facilitate cross border co-operation.

**Cross-border enforcement against SPAM requires a global strategy to reach effectiveness**

If national co-ordination is a prerequisite for international co-operation, enforcement action across borders would still benefit from a global strategy to overcome a number of challenges to information gathering and sharing, to identify enforcement priorities, and to develop an effective international enforcement framework.

Adequate mechanisms for information gathering and sharing are needed for enforcement agencies to be able to investigate, preserve and obtain information and evidence and share that information with foreign counterparts in appropriate circumstances. It may be that cross border co-operation would have its greatest potential for success when authorities in the country of origin respond to the request of an authority in the recipient country because authorities in the country where a SPAMmer is located are generally in a better position to identify the person behind an account from which SPAM was sent. If so, enforcement agencies in countries where SPAM is received should endeavor to locate the SPAMmers and provide evidence enabling the authority in the country where the SPAM originates to exercise its powers, and, for example, compel production of information.

As no country can be expected to investigate and take action in response to every request from a foreign authority, it may be appropriate to establish priorities regarding what types of complaints are most appropriate for cross border co-operation. Despite the differing approaches to legislating against SPAM, and in particular the “opt-in” vs. “opt-out”, it appears that a considerable volume of SPAM would be illegal under most of the current legal frameworks. The real challenge is to move towards a common approach to prioritising[38] which cases are worthy of the considerable effort required to bring actions in cross-border cases.

[38] There are many possible different grounds for granting priority to a SPAM compliant. Multiple factors might be considered in the scene such as the content of the message, the degree of damage, the false or deceptive claims in the message, etc. The most commonly used criteria by OECD countries are based on the type of damage the message may cause, e.g. risk to the financial or health interests of consumers, user privacy and damage to networks and property. The type of spam most commonly identified as being an appropriate priority for cross-border co-operation is e-mail containing false or deceptive claims causing damage to the recipient.

Finally, further consideration of how best to develop effective frameworks and arrangements for international co-operation would be important. The range of options is wide: further informal frameworks such as bilateral MOUs[39], multilateral or model MOUs, networks such as the London Action Plan, formal frameworks such as the OECD Guidelines on Cross-border Fraud, or binding legal instruments such as the Council of Europe Cybercrime Convention. While informal frameworks do indeed improve communication and working-level collaboration, a formal framework may be more appropriate in the future to create a common stable and effective mechanism at global level. Such a framework would not need to be all inclusive, but could constitute the basis for further/enlarged arrangements among interested players, and be a platform for the various initiatives currently planned or developed.

#### Global outreach should be the objective

One of the major risks to effective enforcement of anti-SPAM laws is the ease with which SPAMmers may set-up their operations and move to jurisdictions where there is no anti-SPAM law, where the enforcement capacity is weak and international co-operation is laden with conditions. Such jurisdictions may be the weakest link. To avoid the creation of SPAM havens, efforts to strengthen capacity to take action against SPAMmers should reach out to the broadest possible coalition of enforcement agencies worldwide.

### 4.7.2 ITU

During the 2003 Global Symposium for Regulators a recommendation was made that the ITU launch a discussion on frameworks for international cooperation on countering SPAM. Following this recommendation a virtual conference on regulatory cooperation on SPAM was held at the end of March. In addition, ITU decided to hold a WSIS Thematic Meeting on Countering SPAM, to gather all interested stakeholders and discuss possible international cooperative solutions to this scourge. The meeting gathered representatives from about 60 governments, and allowed, for the first time, participants from less developed economies to express their concerns and their needs in this field. Among the several contributions made to the meeting, a special note should be made of the intervention of a group of developing countries, who affirmed the importance of raising awareness on the problems they are encountering with SPAM and the need to have fora in which they could exchange information and experiences.

Developing countries called for more support from developed countries and the international community in facing the problem of SPAM in particular, and Internet security in general, recognizing that, while legislation in itself is not the solution, it could indeed help in fighting this phenomenon. Their suggestion for the creation of an effective framework for international

[39] Examples of such MoUs and bilateral/multilateral agreements can be found here:

- LAP: http://www.londonactionplan.org/?q=node/1
- MoUs:
    - ACCC, ACA (Australia), OFT, ICO (United Kingdom), FTC (United States) http://www.ftc.gov/os/2004/07/040630spammoutext.pdf
    - ACA (Australia), NOIE (Australia), KISA (Korea) http://www.acma.gov.au/acmainterwr/consumer_info/spam/spam_mou.rtf
    - DCITA (Australia), MICT (Thailand) http://www.itu.int/osg/spu/spam/legislation/aust_thailand_joint_statement.rtf
    - Seoul-Melbourne http://www.acma.gov.au/acmainterwr/consumer_info/frequently_asked_questions/spam-multilateral_mou-seoul-melbourne_agreement-draft.pdf

cooperation and coordination--with the active participation of developing countries, was warmly supported.

Following the conclusion of the meeting, ITU is continuing its work on countering SPAM, elaborating a database gathering laws, information and contact details of enforcement authorities dealing with SPAM worldwide, cooperating with other international organizations in areas of common interest, and promoting the creation of a suitable framework for international cooperation, which could lead to the adoption of a global agreement on the subject.

### 4.7.3 WORKING GROUP ON INTERNET GOVERNANCE (WGIG)[40]

The main activity of the Working Group on Internet Governance (WGIG) is to investigate and make proposals for action, as appropriate, on the governance of Internet.

WGIG established public policy areas for the issues relating to the use of the Internet, including SPAM, network security and cybercrime.

WGIG has published on the 5th of June 2005 the "Background Report: The Working Group on Internet Governance" and the actual "Report of the Working Group on Internet Governance. The WGIG devoted much of its attention to the identification of public policy issues that are potentially relevant to Internet governance, including SPAM. Based on their findings, the WGIG established key public policy areas including SPAM, network security and cybercrime.

Among their recommendations focused on governance mechanisms, WGIG outlines that standardization of software or procedures as a key element in dealing with SPAM.

### 4.7.4 MESSAGING ANTI-ABUSE WORKING GROUP (MAAWG)

#### Principles of the Code of Conduct:

MAAWG has developed a set of characteristics to be considered in a code of conduct as an international initiative for all messaging providers as follows:

- Messaging operators should provide end users with a policy document (e.g., Acceptable Use Policy), which defines permissible/prohibited uses of the messaging services.
- Messaging operators shall make reasonable efforts to hold customers accountable to the network's Acceptable Use Policy. Patterns of abuse that emanate from an operator's network should be a concern to that operator and its customer(s) to resolve in a timely manner.
- Downstream receivers have the right to protect their servers, networks, users and other applicable resources from abuse by other operator's systems. In exercising this right, they may take action that prevents abusive messaging systems from accessing their resources. Decisions to implement protective measures to prevent access or provide reduced access to a particular messaging operator's resources should be based on evaluating the need to protect those resources with the desire to deliver quality messaging service to an operator's users.
- Messaging operators should make reasonable efforts to communicate with other operators regarding abuse issues via manual or automated methods to address implementation of "protective measures".

[40] *Source: Working Group on Internet Governance (WGIG). On (www.wgig.org/).*

**Note 1:** The code addresses messaging from a particular sender to a defined group of recipients and is not explicitly meant to apply to those Internet institutions for the publishing of messages to a generalized audience that is self-selected, such as Usenet or Listservs.

**Note 2:** The Code's principles may further be supported by the MAAWG Best Practices document, if and when developed and approved. The Best Practices document is intended to highlight technical implementations and operational recommendations for the principles of the Code.

**Note 3:** The Code is not meant to supplant, supersede, or otherwise replace any accepted standard of the IETF. It should be interpreted and applied in conformity with relevant rules of international law, laws of individual Nations, States, or Sovereignties in which messaging operators function, and Internet standards.

### 4.7.5 ANTI-PHISHING WORKING GROUP (APWG)

**Specific Technical and Business Recommendations:**

The Best Practices outline technology and business methods that will help ISPs maintain cleaner communications channels for their customers and protect their infrastructures from interlopers seeking to commandeer the network. In addressing the deployment of security technologies, the paper encourages piloting and field trials of technologies and comparative analysis of multiple solutions. Among the recommendations:

- Two way filtering of communications flows to stop inbound phishing email from reaching consumers and to tip off ISPs and mailbox providers when their servers are being used for sending outbound phishing emails.
- Internet Protocol (IP) blacklists to temporarily render servers co-opted for phishing attacks unreachable by consumers caught up in a scam; using URL-based filters to help ISPs filter their customer traffic outbound to IP addresses, domains or URLs where known phishing Web pages are hosted.
- Filtering or rejecting email if it can be unequivocally determined to be forged; disabling images and hyperlinks in email from untrusted sources.
- Employing visual cues or tags within the email client interface that can characterize the authenticity and trustworthiness of email for the users.
- Blocking access to known phishing sites during attacks and distributing client tools that users can employ to deflect their Web browser from accessing phishing sites.

### 4.7.6 THE ASIA PACIFIC COALITION AGAINST UNSOLICITED (APCAUCE)[41]

APCAUCE is the Asia Pacific wing of CAUCE, the Coalition Against Unsolicited Commercial Email. CAUCE is the world's largest volunteer anti-SPAM organization, with chapters in the USA, Canada, the EU and over a dozen economies in the Asia Pacific region.

[41] *Source: The Asia Pacific Coalition Against Unsolicited (APCAUCE). On (www.apcauce.org/).*

APCAUCE is an all volunteer coalition of internet users, email service providers, internet service providers, academic, and legislation parties. They meet twice every year to share best practices and updated news of each region, to reconfirm their opposition to the threat of resources that Unsolicited Commercial Email (UCE) represents, and to form active agenda against UCE that best fit each region.

# APPENDIX A: INTERNATIONAL BODIES AND INITIATIVES

## 1. The International Telecommunication Unions (ITU)

Introduction

The International Telecommunication Union (ITU) is an international organization established to standardize and regulate international radio and telecommunications. ITU promotes the exchange of information and best practices and provides support to developing countries.

Membership

ITU is headquartered in Geneva, Switzerland. It is an international organization within the United Nations System where governments and the private sector coordinate global telecom networks and services. It is comprised of 191 state members from across the globe, and it has 3 sectors, namely the Radio communication sector, Standardization sector, and the Development sector. Saudi Arabia is a member in ITU.

The work of the ITU is conducted by its members. As part of the United Nations structure, a country can be a member, in which case it is referred to as a Member State. Companies and other such organizations can hold other classes of membership referred to as Sector Member or Associate status. Sector and Associate memberships enable direct participation by a company in the development of standards (something not allowed in some other standards bodies such as ISO, where formal ballots are processed by a single entity per country and companies participate only indirectly through national delegations). Various parts of the ITU also maintain liaison relationships with other organizations. Members are the Vatican City and almost all of the UN members.

Field of Interest

ITU created an informal network of regulators and policy makers operating in the field of anti-SPAM activities, providing reliable information and data, and offering a platform to facilitate discussion and exchange of experiences. Moreover, ITU provides whitepapers, and documents related to SPAM. ITU concentrates on several aspects anti-SPAM. This includes regularity approach, enforcement cooperation, industry driven activities, technical solution, education and awareness, and international cooperation.

Contact Information

Website: http://www.itu.int

Postal Address:

ITU
Place des Nations

CH-1211 Geneva 20
Switzerland

Telephone: +41 22 730 51 11

## 2. The Organization for Economic Co-operation and Development (OECD)

Introduction

The Organization for Economic Co-operation and Development (OECD) is an international organization of those developed countries that accept the principles of representative democracy and a free market economy.

Membership

The OECD groups 30 member countries sharing a commitment to democratic government and the market economy. With active relationships with some 70 other countries and economies, Non Government Organizations (NGOs) and civil society, it has a global reach.

Twenty countries originally signed the Convention on the Organization for Economic Co-operation and Development on 14 December 1960. Since then a further ten countries have become members of the Organization. The Member countries of the Organization and the dates on which they deposited their instruments of ratification are:

- AUSTRALIA: 7 June 1971;
- AUSTRIA: 29 September 1961;
- BELGIUM: 13 September 1961;
- CANADA: 10 April 1961;
- CZECH REPUBLIC: 21 December 1995;
- DENMARK: 30 May 1961;
- FINLAND: 28 January 1969;
- FRANCE: 7 August 1961;
- GERMANY: 27 September 1961;
- GREECE: 27 September 1961;
- HUNGARY: 7 May 1996;
- ICELAND: 5 June 1961;
- IRELAND: 17 August 1961;
- ITALY: 29 March 1962;
- JAPAN: 28 April 1964;
- KOREA: 12 December 1996;
- LUXEMBOURG: 7 December 1961;
- MEXICO: 18 May 1994;
- NETHERLANDS: 13 November 1961;
- NEW ZEALAND: 29 May 1973;
- NORWAY: 4 July 1961;
- POLAND: 22 November 1996;
- PORTUGAL: 4 August 1961;

- SLOVAK REPUBLIC: 14 December 2000;
- SPAIN: 3 August 1961;
- SWEDEN: 28 September 1961;
- SWITZERLAND: 28 September 1961;
- TURKEY: 2 August 1961;
- UNITED KINGDOM: 2 May 1961; and
- UNITED STATES: 12 April 1961.

Field of Interest

OECD is best known for its publications and its statistics, its work covers economic and social issues from macroeconomics, to trade, education, development and science and innovation. It plays a prominent role in fostering good governance in the public service and in corporate activity, and helps governments to ensure the responsiveness of key economic areas with sectoral monitoring. By deciphering emerging issues and identifying policies that work, it helps policy-makers adopt strategic orientations. It is well known for its individual country surveys and reviews, internationally agreed instruments, decisions and recommendations to promote rules of the game in areas where multilateral agreement is necessary for individual countries to make progress in a globalize economy.

OECD had developed an anti-SPAM toolkit of recommended policies and measures to combat SPAM. This includes regularity approach, enforcement cooperation, industry driven activities, technical solution, education and awareness, SPAM measurement, and international cooperation.

Contact Information

Website: http://www.oecd.org

Postal Address: OECD 2, rue André Pascal, F-75775 Paris Cedex 16, France

Telephone: +33 145248200

Fax: +33 145248500

## 3. SPAMHAUS

Introduction

The SPAMHAUS Project is an international non-profit organization whose mission is to track the Internet's SPAM Gangs, to provide dependable real-time anti-SPAM protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue Spammers worldwide, and to lobby governments for effective anti-SPAM legislation.

Membership

Founded in 1998, SPAMHAUS is based in Geneva, Switzerland and London, UK and is run by a dedicated team of 25 investigators and forensics specialists located in 9 countries.

Field of Interest

SPAMHAUS combats SPAM from two aspects. It provides technical solution, and awareness and education. SPAMHAUS publishes the Register Of Known SPAM Operations (ROKSO) - a database collating information and evidence on the '200' known worst SPAM gangs worldwide, used by ISPs to avoid signing up known Spammers who would abuse their networks and by Law Enforcement Agencies to help target and mount prosecutions against professional Spammers.

SPAMHAUS publishes a number of real-time SPAM-blocking databases, including the SPAMHAUS Block List (SBL), the Exploits Block List (XBL) and the Policy Block List (PBL). Broadcast from a network of 40 DNS servers in 17 countries, the SPAMHAUS blacklists are used by many of the Internet's major Internet Service Providers, Corporations, Universities, Governments and Military networks.

Contact Information

Website: http://www.SPAMHAUS.org

Email: admin-eu@SPAMHAUS.org

## 4. Seoul-Melbourne Anti-SPAM Agreement

Introduction

Seoul-Melbourne Anti-SPAM Agreement consists of twelve Asia-Pacific communications and Internet agencies that have joined the Australian Communications Authority (ACA) and the Korean Information Security Agency (KISA) in signing the Seoul-Melbourne Anti-SPAM Agreement, a multilateral memorandum of understanding (MoU) on cooperation in countering SPAM. The MoU is focused on sharing knowledge, information and intelligence about known sources of SPAM, network vulnerabilities, methods of SPAM propagation, and technical, education and policy solutions to the SPAM problem.

Membership

- Twelve Asia-Pacific communications and Internet agencies have joined the Australian Communications Authority in signing a memorandum of understanding -- the Seoul-Melbourne Anti-SPAM Agreement -- on cooperation in countering SPAM;
- Australian Communications Authority (ACA);
- Korea Information Security Agency (KISA);
- Internet Society of China (ISC);
- Commerce, Industry and Technology Bureau, Hong Kong (CITB);
- National computer centre (NCC) of the Philippines;
- Philippines Computer Emergency Response Team (PH-CERT);
- Malaysian Communications and Multimedia Commission (MCMC);
- Ministry of Economy, Trade and Industry, Japan (METI);
- Ministry of Internal Affairs and Communications (MIC) Japan;
- Ministry of Information and Communication Technology, Kingdom of Thailand (MICT);
- New Zealand Ministry of Economic Development (MED); and
- Taiwan Computer Emergency Response Team/Coordination Centre Information.

Field of Interest

This MoU is concerned with the international cooperation between organizations to fight SPAM.

Contact Information

Postal address:

Level 44, Melbourne Central Tower,

360 Elizabeth Street, Melbourne

VIC 3000 Australia

Telephone: + 61 3 9963 6736

Fax: + 61 3 9963 6957

Email: meg.mundell@aca.gov.au

## 5. Working Group on Internet Governance (WGIG)

Introduction

The Working Group on Internet Governance (WGIG) is a United Nations multi stakeholder working group set up after the 2003 World Summit on the Information Society (WSIS) first phases Summit in Geneva to agree on the future of Internet governance.

Membership

This working group has various members from around the world. Their members are usually qualified academics and professionals in various fields related to ICT.

Field of Interest

The main activity of the WGIG is to investigate and make proposals for action, as appropriate, on the governance of Internet. WGIG established public policy areas for the issues relating to the use of the Internet, including SPAM, network security and cybercrime. While these issues are directly related to Internet governance, the nature of global cooperation required is not well defined. It is important to note that OECD works on WGIG-designated public policy issues because many of the priority issues for the WGIG are also priority areas for the OECD.

Contact Information

Website: https://www.wgig.org

Postal Address:

United Nations

Secretariat of the Working Group on Internet Governance

Palais des Nations, CH-1211 Geneva 10

Switzerland
Telephone: +41 22 917 57 68

Fax: +41 22 917 00 92

Email: wgig@unog.ch

## 6. Asia-Pacific Economic Cooperation Telecommunications & Information Working Group (APEC)

Introduction

APEC TEL WG is the Asia-Pacific Economic Cooperation Telecommunications & Information Working Group. The Telecommunications & Information Working Group (TEL WG) is committed to improving the telecommunications and information infrastructure in the region and to facilitating effective cooperation, free trade and investment and sustainable development. It was formed in 1989.

Membership

APEC has 21 members. The word 'economies' is used to describe APEC members because the APEC cooperative process is predominantly concerned with trade and economic issues, with members engaging with one another as economic entities.

Field of Interest

The TEL's program of action covers different activities including: E-security, E-government, and hosting meetings and conferences regarding SPAM. Its focus in combating SPAM is on ensuring international cooperation against SPAM.

Contact Information

Website: http://www.apec.org

Postal Address:

APEC Secretariat

35 Heng Mui Keng Terrace,

Singapore 119616

Telephone: (65) 6775 6012

Fax: (65) 6775 6013

## 7. The Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE)

Introduction

APCAUCE is the Asia Pacific wing of CAUCE, the Coalition Against Unsolicited Commercial Email. CAUCE is the world's largest volunteer anti-SPAM organization, with chapters in the USA, Canada, the EU and over a dozen economies in the Asia Pacific region.

Field of Interest

APCAUCE is concerned with providing education awareness and international cooperation against combating SPAM.

Contact Information

Website: http://www.apcauce.org

Email: chair@apcauce.org

## 8. The Anti-Phishing Working Group (APWG)

Introduction

The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing and the spread of crimeware that automatically mines consumers' personal data from their PCs.

Membership

Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. There are currently over 1500 organizations participating in the APWG and more than 2400 members worldwide. The APWG maintains a public website for its members and for the general public.

Field of Interest

APWG is concerned with providing technical solutions. The organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks. APWG provides a Report-Phishing service by building a repository of phishing scam emails and websites to help people identify and avoid being scammed in the future. Moreover, they provide technical whitepapers and briefings from APWG Sponsors, such as: McAfee, Symantec and RSA Security.

Contact Information

Website: http://www.antiphishing.org

Email: info@antiphishing.org

## 9. Messaging Anti-Abuse Working Group (MAAWG)

Introduction

Messaging Anti-Abuse Working Group (MAAWG) is a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. MAAWG is where the messaging industry comes together to work against SPAM, viruses, denial-of-service attacks and other online exploitation. MAAWG addresses messaging abuse by systematically engaging all aspects of the problem. This includes technology, industry collaboration and public policy. The MAAWG is a group of telecommunications companies brought together by OpenWave[42] in early 2004.

Field of Interest

The purpose of the group is to fight SPAM, phishing, and other possible forms of e-mail abuse. MAAWG SPAM-related activities & services include:

- Getting the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging SPAM;
- Running Anti-SPAM workshops; and
- MAAWG worked together with the OECD Anti-SPAM Task Force & developed an E-mail Metrics Program and agreed on a series of ISPs SPAM indicators.

[42] A commercial provider of software solutions for the communications and media industries

Contact Information

Website: http://www.maawg.org

## 10. The Internet Engineering Task Force (IETF)

Introduction

The Internet Engineering Task Force (IETF) develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standard bodies. The IETF is formally an activity under the umbrella of the Internet Society. Request for Comments (RFCs) are a series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies.

Field of Interest

IETF is concerned with industry driven activities and awareness of SPAM. Two Examples of relevant RFCs are: RFC 2635 and RFC 2505.

- RFC 2635: A Set of Guidelines for Mass Unsolicited Mailings and Postings (SPAM*). This RFC was produced in June 1999; and
- RFC 2505: Anti-SPAM Recommendations for SMTP MTAs. This RFC was produced in February 1999.

Contact Information

Website: http://www.ietf.org

Postal Address: IETF Secretariat, c/o NeuStar, Inc.

Corporate Headquarters: 46000 Center Oak Plaza, Sterling, VA 20166

Phone: +1-571-434-3500

Fax: +1-571-434-3535

Email: ietf-info@ietf.org

## 11. London Action Plan (LAP)

Introduction

LAP is an international action plan designed to encourage communication and cooperation between countries in tackling SPAM and SPAM-related problems.

On October 11, 2004, government and public agencies from 27 countries responsible for enforcing laws concerning SPAM met in London to discuss international SPAM enforcement cooperation. At this meeting, a broad range of SPAM enforcement agencies, including data protection agencies, telecommunications agencies and consumer protection agencies, met to discuss international SPAM enforcement cooperation. Several private sector representatives also collaborated in parts of the meeting.

Membership

The London Action Plan (LAP) conference was hosted in 2004 by the Office of Fair Trading (OFT) from the United Kingdom and the US Federal Trade Commission (FTC) from the United States. It brings together agencies from different countries to promote cross-border cooperation on spam and spam-related problems, such as on-line fraud and computer viruses. The members are either government agencies or industry participants. Next is a list of all the members in the LAP.

Members are:

GOVERNMENT AGENCIES

- Australia: Australian Communications & Media Authority (ACA) and Australian Competition and Consumer Commission (ACCC);
- Belgium: DG Enforcement and Mediation of the Federal Public Service Economy and Federation of European Direct and Interactive Marketing;
- Canada: Industry Canada Office of the Privacy Commissioner of Canada;
- Chile:National Consumer Service (SERNAC);
- China: Union Network Beijing;
- Denmark: Office of the Danish Consumer Ombudsman;
- Finland: Finnish Consumer Agency and Ombudsman;
- Hungary: General Inspectorate for Consumer Protection of Hungary, Department of EU Coordination, General Inspectorate for Consumer Protection of Hungary, Directorate of Informatics Regulation;
- Ireland: Data Protection Commissioner;
- Japan: Ministry of Internal Affairs and Communications, Telecommunications Bureau, Telecommunications Business Department, Telecommunications Consumer Policy Division, Japan Fair Trade Commission (JFTC);
- Latvia: Consumer Rights Protection Centre;
- Lithuania: Communications Regulatory Authority of the Republic of Lithuania;
- Malaysia:National ICT Security and emergency Response Centre (NISER), Malaysia Communications and Multimedia Commission;
- Mexico: Procuraduria Federal del Consumidor, Comision Federal de Telecomunicaciones;
- Nigeria: Economic and Financial Crimes Commission;
- Norway: Norwegian Consumer Ombudsman;
- Republic of Korea: Korean Information Security Agency (KISA), Korea Consumer Protection Board;
- Spain: Spanish Data Protection Agency;
- Sweden: The Swedish Consumer Agency/Consumer Ombudsman;
- Switzerland: State Secretariat for Economic Affairs SECO;
- Taiwan: Ministry of Transportation and Communications, Taiwan Network Information Centre;
- The Netherlands: Independent Post & Telecommunication Authority;

- UK: Office of Fair Trading (OFT), Information Commissioner Office (ICO), LACORS; and
- USA: US Federal Trade Commission (FTC).

INDUSTRY PARTICIPANTS

- Australia: (Spammatters);
- Belgium (FEDMA);
- Chile (Chilean ISP Association (API), Santiago Chamber of Commerce);
- China (Internet Society of China);
- France (Microsoft EMEA);
- Germany (ECO);
- Hong Kong(Outblaze Limited);
- Malaysia (National ICT Security and Emergency Response Centre (NISER), Digi.com);
- N/A (APCAUCE, CAUCE, Vircom,);
- Spain (Telefonica);
- UK (Microsoft EMEA, LINX, ISPA UK, MessageLabs, Checkbridge, The Spamhaus Project, Nominet UK, Wanadoo UK plc); and
- USA (Verizon Online, Latham & Watkins LLP (for AOL), McAfee).

Field of Interest

The purpose of this Action Plan is to promote international SPAM enforcement cooperation and address SPAM related problems, such as online fraud and deception, phishing, and dissemination of viruses.

Contact Information

Website: http://www.londonactionplan.com

Email: admin@londonactionplan.com

## 12. GSM Association

Introduction

The GSM Association (GSMA) is a global trade association. The primary goals of the GSMA are to ensure mobile phones and wireless services work globally and are easily accessible, enhancing their value to individual customers and national economies, while creating new business opportunities for operators and their suppliers.

Membership

Members of GSMA include GSM mobile phone operators, manufacturers, and suppliers. These members support the Association's initiatives as associate members.

Associate membership can be held by a corporate group or by an independent legal entity of a corporate group but not an individual. Whether an associate membership is held by an independent legal entity of a corporate group or by the whole corporate group, GSM Association information must be limited to direct employees only.

There are currently 14 categories of Associate Membership:

- Application Providers;
- Billing Systems Suppliers;
- Data Clearing Houses;
- Financial Clearing Houses;
- GRX Carriers;
- GSM Standards Supporter;
- Infrastructure Supplier;
- International Transit Carrier;
- Mobile Terminal Suppliers;
- Roaming Brokers;
- Security Systems Suppliers;
- Signaling Providers;
- SIM Card Suppliers; and
- Simulators Suppliers.

Field of Interest

The GSMA plays a pivotal role in the development of the GSM platform and the global wireless industry. Much of the GSMA's work is focused on two areas: Emerging services and emerging markets. The GSMA helps its members develop and launch new services, ranging from mobile instant messaging to video sharing to mobile Internet access, which will work across networks and across national boundaries. At the same time, the GSMA is heavily engaged in the industry’s push to extend basic voice and text services to more people in emerging markets. GSMA had developed a code of conduct addressing mobiles SPAM.

Contact Information

Website: http://www.gsmworld.com

## 13. Mobile Marketing Association

Introduction

The Mobile Marketing Association (MMA) is the premier global association that strives to stimulate the growth of mobile marketing and its associated technologies. It is the primary source for mobile marketing information and expertise.

Membership

The MMA is a global organization with 400 members representing over twenty countries. MMA members include agencies, advertisers, hand held device manufacturers, carriers and operators, retailers, software providers and service providers, as well as any company focused on the potential of marketing via mobile devices.

The Mobile Marketing Association offers membership in a variety of categories based on member size as well as geography. All members joining at the global and regional level will receive the most extensive set of member benefits. Individual and academic membership have varies membership benefits which are detailed below. The region in which the MMA currently has operations includes:

- North America (NA);
- Europe, Middle East & Africa (EMEA);
- Asia Pacific (APAC); and
- Central & Latin America (CALA) - under development, launch in Q2-07.

Field of Interest

MMA had developed a code of conduct for addressing mobile SPAM. MMA is dedicated to:

- Providing an industry forum to meet, discuss, plan and work cooperatively to resolve key industry issues.
- Bringing together industry-wide, global and regional work groups that focus on industry initiatives.
- Providing representation for the mobile marketing industry to major legislative bodies worldwide.
- Sharing perspectives on mobile marketing between Europe, Asia, Latin America, Africa and the U.S.
- Fueling peer-to-peer interaction through seminars, conferences and events.
- Developing metrics for measuring ad delivery and consumer response.
- Developing open and compatible mobile marketing technical and creative standards.
- Defining and publishing mobile marketing best practices and guidelines on privacy, ad delivery, and ad measurement.
- Providing the value and effectiveness of mobile marketing to advertisers, agencies and consumers.
- Serving as the key advocate on behalf of the mobile marketing industry.

Contact Information

Website: http://www.maaglobal.com

## 14. Regional Entities/Bodies

The following regional entities and bodies will be considered as applicable:

- The Arab League: The Arab league is an association of Arab states established in 1945 to promote cooperation among member nations in matters relating to economic and social development and foreign policy. Numerous specialized organizations and other institutions that promote Arab cooperation and protect Arab interests in a wide array of fields fall under the league umbrella. One of the specialized organizations in this association is the Arab Telecommunications Union.

- The Gulf Cooperation Council (GCC): The GCC seeks to promote coordination between member states in the Arab Gulf in all fields in order to achieve unity.
- The Arab ICT Regulators' Network: The Arab ICT Regulators' Network is an independent organization created at the ITU's first Arab Regulators meeting in Algiers in April 2003, with the objective of sharing experiences and developing expertise that will enable Arab ICT regulators to facilitate growth in telecom products and services and achieve equality of access to such services and products in the Arab region.

## 15. Messaging Providers

Messaging providers provide email services accessible from a Web browser anywhere in the world. They offer free accounts worldwide with features such as SPAM filters and enhanced virus scanning. Moreover, they offer SPAM reporting service, SPAM monitoring and statistics.

The following messaging providers will be considered as applicable:

- Yahoo;
- Hotmail; and
- Gmail.

# APPENDIX B: SAMPLES OF EXISTING MOUS AND INTERNATIONAL AGREEMENTS

This section lists few of the already existing MoUs and International Agreements which were taken as they are from the available sources.

## MEMORANDUM OF UNDERSTANDING ON MUTUAL ENFORCEMENT ASSISTANCE IN COMMERCIAL EMAIL MATTERS AMONG AGENCIES OF THE UNITED STATES, THE UNITED KINGDOM, AND AUSTRALIA.

The U.S. Federal Trade Commission ("FTC"), Her Majesty's Secretary of State for Trade and Industry in the United Kingdom ("Secretary of State"), the Office of Fair Trading in the United Kingdom ("OFT"), the United Kingdom's Information Commissioner, the Australian Competition and Consumer Commission ("ACCC"), and the Australian Communications Authority ("ACA"),

RECOGNISING that the convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial email which often contains deceptive content or material that many recipients may consider offensive in nature;

RECOGNISING the challenges posed by the proliferation of commercial email in each Participant's country, and desiring to improve the effectiveness of the enforcement of certain provisions of the Commercial Email Laws of their respective countries while also recognizing the importance of freedom of expression;

RECOGNISING that the Commercial Email Laws and the methods of enforcing such laws differ substantially among the countries, in particular as to the role played by local and/or regional enforcement authorities;

RECOGNISING that there is a need to ensure that appropriate local and/or regional enforcement authorities with whom Evidence is shared under this Memorandum are made fully aware of the terms of this Memorandum and are encouraged to cooperate with the Participants in so far as they are permitted to do so by their respective national laws, enforcement policies and other important interests, consistent with the terms of this Memorandum;

RECOGNISING that the laws of their respective countries contain certain restrictions on international law enforcement assistance, including information disclosure, and that nothing in this Memorandum requires the Participants to provide assistance if such assistance is prohibited by their respective national laws, enforcement policies and other important interests;

RECOGNISING that the FTC, the OFT, and the Secretary of State want to build upon the mutual enforcement assistance provided for in the MEMORANDUM OF UNDERSTANDING ON MUTUAL ENFORCEMENT ASSISTANCE IN CONSUMER PROTECTION MATTERS BETWEEN THE FEDERAL TRADE COMMISSION OF THE UNITED STATES OF AMERICA AND HER MAJESTY'S SECRETARY OF STATE FOR TRADE AND INDUSTRY AND THE DIRECTOR GENERAL OF FAIR TRADING IN THE UNITED KINGDOM dated October 31, 2000;

RECOGNISING that the FTC and the ACCC want to build upon the mutual enforcement assistance provided for in the AGREEMENT BETWEEN THE FEDERAL TRADE COMMISSION OF THE UNITED STATES OF AMERICA AND THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION ON THE MUTUAL ENFORCEMENT ASSISTANCE IN CONSUMER PROTECTION MATTERS dated July 17, 2000; and

RECOGNISING that the OFT, the Secretary of State, and the ACCC want to build upon the cooperation provided for in the COOPERATION ARRANGEMENT BETWEEN THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION, THE COMMERCE COMMISSION IN NEW ZEALAND AND HER MAJESTY'S SECRETARY OF STATE FOR TRADE AND INDUSTRY AND THE OFFICE OF FAIR TRADING IN THE UNITED KINGDOM REGARDING THE APPLICATION OF THEIR COMPETITION AND CONSUMER PROTECTION LAWS dated October 16, 2003,

HAVE REACHED THE FOLLOWING UNDERSTANDINGS:

I: Definitions

For the purposes of this Memorandum,

A. "Commercial Email Laws" means

1. in the case of the United States: (a) the CAN-SPAM Act of 2003; and (b) any other laws enforced by the Federal Trade Commission that would prohibit unfair or deceptive acts or practices in connection with commercial email, including Section 5 of the Federal Trade Commission Act;

2. in the case of the United Kingdom: (a) the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Data Protection Act 1998, and the Electronic Commerce (EC Directive) Regulations 2002; and (b) any other laws enforced by the Office of Fair Trading that would prohibit unfair or deceptive acts or practices in connection with commercial electronic communications, as listed in Annex A to this Memorandum; and

3. in the case of Australia: (a) Parts IVA, V, and VC of the Trade Practices Act of 1974; (b) the Spam Act 2003; and (c) the Telecommunications Act 1997;

as well as any amendments thereto, and such other laws or regulations as the Participants may from time to time decide in writing to be a Commercial Email Law for purposes of this Memorandum. The FTC, the Secretary of State, the ACCC and the ACA should promptly notify the other Participants of any relevant amendments to their Commercial Email Laws.

B. "Evidence" means information, testimony, statements, documents or copies thereof, or other things, that are lawfully obtained in anticipation of or during the course of an investigation or proceeding under the Participants' respective Commercial Email Laws.

C. "Participant" means

1. in the case of the United States, the FTC;

2. in the case of the United Kingdom, the Secretary of State, the OFT, or the Information Commissioner, acting with respect to their respective enforcement responsibilities under the Commercial Email Laws as here defined; and

3. in the case of Australia, the ACCC or the ACA acting with respect to their respective enforcement responsibilities under the Commercial Email Laws as here defined.

D. "Person" means any natural person or legal entity, including corporations, unincorporated associations, partnerships, or bodies corporate existing under or authorized by the laws of: (i) the Territories (as defined below) of the United States, the United Kingdom, or Australia; or (ii) other sovereign states.

E. "Request" means a request for assistance under this Memorandum.

F. "Requested Participant" means the Participant from which assistance is sought under this Memorandum, or which has provided such assistance.

G. “Requesting Participant” means the Participant seeking or receiving assistance under this Memorandum.

H. “Spam Violations” means conduct prohibited by a country’s Commercial Email Laws that is substantially similar to conduct prohibited by the Commercial Email Laws of the other countries, including, but not necessarily limited to:

1. sending commercial email containing deceptive content;

2. sending commercial email without providing the recipient with a means, such as a valid email address or an Internet based mechanism, to request that such communications cease;

3. sending commercial email that contains misleading information about the message initiator, or fails to disclose the sender’s address; or

4. sending commercial email, when the recipient has specifically requested the sender not to do so.

I. “Territory” means:

1. in the case of the United States: the United States, its States, its Territories, and the District of Columbia;

2. in the case of the United Kingdom: the United Kingdom, its Overseas Territories and Crown Dependencies; and

3. in the case of Australia: Australia, its States, and its Territories.

II: Object and Scope of Assistance

A. The Participants recognize that it is in their common interests to share Evidence that will: facilitate effective enforcement against Spam Violations; avoid unnecessary duplication; facilitate sequential, simultaneous or coordinated investigations of Spam Violations or suspected Spam Violations; facilitate research and consumer and business education; promote a better understanding by each of economic and legal conditions and theories relevant to enforcement against their respective Spam Violations and related activities; and keep each other informed of developments in their respective countries having a bearing on this Memorandum.

B. In furtherance of this common interest, and subject to Paragraph IV, the Participants intend to use best efforts to exchange and provide appropriate information in relation to: consumer and business education; investigations and research in relevant areas, including the practices of address harvesting and dictionary attacks; speeches; research papers; journal articles; compliance education programs; self regulatory and technical enforcement solutions; amendments to relevant legislation; and staffing and resource issues, including the possibility of staff exchanges and visits.

C. Subject to Paragraphs II.F and IV, the Participants intend to use best efforts to assist one another and to cooperate on a reciprocal basis

1. in providing or obtaining Evidence that could assist in determining whether a Person has committed or is about to commit a Spam Violation; or

2. in facilitating the administration or enforcement against Spam Violations.

D. Subject to Paragraph IV, the Participants intend to use their best efforts to inform each other as soon as practicable about Spam Violations occurring or originating in the Territory of the United States, the United Kingdom, or Australia, or that affect consumers in the Territory of the United States, the United Kingdom, or Australia.

E. Subject to Paragraph IV, assistance contemplated by this Memorandum includes, but is not limited to:

1. using best efforts to disclose, provide, exchange, or discuss Evidence in the possession of any Participant;

2. using best efforts to cooperate in the detection and investigation of Spam Violations;

3. using best efforts to obtain, or arrange the obtaining of Evidence at the request of a Participant, including

a. taking the testimony or statements of Persons or otherwise obtaining information from Persons;

b. obtaining documents, records or other forms of documentary Evidence; or

c. locating or identifying Persons or things;

4. using best efforts to assist in service of process;

5. using best efforts to share appropriate information provided in complaints by users; and

6. in appropriate cases, coordinating enforcement against cross-border Spam Violations.

F. The Participants recognize that it is not feasible for a Participant to offer assistance to the other Participants for every Spam Violation. Accordingly, the Participants intend to use best efforts, subject to Paragraph IV, to seek and provide cooperation focusing on those Spam Violations most serious in nature, such as those that are causing or may cause injury (financial or otherwise) to a significant number of consumers, and those otherwise affecting particularly large numbers of consumers.

G. Nothing in this Memorandum is intended to prevent a Participant from seeking assistance from or providing assistance to another Participant pursuant to other agreements, treaties, arrangements, or practices.

H. This Memorandum is intended to be used solely for the purpose of law enforcement assistance among the Participants. The provisions of this Memorandum are not intended to give rise to a right on the part of any private person to obtain, suppress, or exclude any Evidence.

I. Nothing in this Memorandum is intended to compel a Person to provide Evidence in violation of any legally applicable right, privilege or restriction.

J. Nothing in this Memorandum is intended to affect any right of a Participant to seek Evidence on a voluntary basis or otherwise lawful basis from a Person located in the Territory of the United States, the United Kingdom or Australia, nor is it intended to preclude any such Person from voluntarily providing Evidence to a Participant.

K. The Participants also intend to use best efforts to promote the wide attendance of government agencies around the world with spam enforcement authorities at the meeting on spam enforcement issues in London in October of 2004, to encourage appropriate subsequent meetings of this nature, and to encourage multi-lateral enforcement cooperation among these agencies with regard to unsolicited commercial email.

III: Requests for Assistance

A. Requests to the FTC should be addressed to: Associate Director, Division of International Consumer Protection, FTC. Requests to United Kingdom Participants should be addressed to the Compliance Manager, Information Commissioner's Office (ICO) and/or the Director of the Consumer Affairs Division in the Office of Fair Trading (OFT), acting on behalf of the OFT's Chairman. The ICO intends to pass Requests on to the Secretary of State or the Office of Fair Trading if the Request relates to legislation for which the Secretary of State or the Office of Fair Trading has enforcement responsibilities. If the ICO passes on a Request to the Secretary of State or the Office of Fair Trading in this way, the Secretary of State or the Office of Fair Trading becomes the Requested Participant for the purposes of this Memorandum, and the ICO should inform the Requesting Participant in writing that the Request has been passed on. The OFT would follow a similar procedure if contacted first. Requests to Australian Participants should be addressed to the Manager, Anti Spam Team, ACA and/or the Chief Executive Officer of the ACCC. The ACA intends to pass Requests on to the ACCC if the Request relates to legislation for which the ACCC has enforcement responsibilities. If the ACA passes on a Request to the ACCC in this way, the ACCC becomes the Requested Participant for the purposes of this Memorandum, and the ACA should inform the Requesting Participant in writing that the Request has been passed on. The ACCC would follow a similar procedure if contacted first.

B. Requests should include:

1. if known, the identification of the Persons subject to any investigation or proceeding;

2. a general description of the subject matter and nature of any investigation or proceeding to which the Request relates;

3. where applicable, a description of the Evidence sought;

4. where applicable, the identity and location of any Person who is to be served with process;

5. where applicable, a description of the action that the Requesting Participant is requesting that the Requested Participant take;

6. where applicable, a description of procedural or evidentiary requirements bearing on the manner in which the Requesting Participant desires the Request to be executed;

7. requirements, if any, for confidential treatment of the Request or its contents; and

8. any other information that the Requesting Participant believes would be helpful in facilitating review or execution of a Request.

C. Requests may also be submitted by completing the International Consumer Protection and Enforcement Network (ICPEN) Information Request Pro Forma.

D. The Participants intend to consult with each other regarding a Request in order to work out details regarding the manner and timing of carrying out the Request.

IV: Limitations on Assistance

A. Consistent with its national laws, international obligations, enforcement policies and other important interests, a Participant should use its best efforts to provide assistance in response to a Request. The Requested Participant may decline to provide assistance.

B. Not withstanding any other provision of this Memorandum, a Participant should not communicate information to the other Participants if such communication is prohibited by the laws of the Participant possessing the information or would be incompatible with that Participant’s important interests.

C. Before denying a Request, the Requested Participant should consult with the Requesting Participant to determine whether assistance may be given in part, subject to specified terms and conditions. If a Request is denied, the Requested Participant should provide the Requesting Participant with a written explanation of the basis for refusal.

D. The determination as to whether to grant a Request in whole or in part rests with: (i) the Associate Director, Division of International Consumer Protection, in the case of the FTC, (ii) either the Secretary of State (or a person acting on his or her behalf), the OFT, or the Information Commissioner (or a person acting on his or her behalf), or (iii) the Chief Executive Officer of the ACCC or the ACA; dependent upon who is the Requested Participant in the case in question.

V: Confidentiality

A. Unless otherwise discussed by the Participants, each Participant should, to the fullest extent possible and consistent with its laws, use its best efforts to maintain the confidentiality of any information communicated to it in confidence by another Participant under this Memorandum.

B. The Requesting Participant may, however, subject to Paragraph IV, communicate such confidential information to other law enforcement agencies within its jurisdiction (having first obtained assurances that best efforts will be used to ensure the maintenance of confidentiality) for the purpose of enforcement against Spam Violations; any such onward sharing of information with other agencies is subject to the consent of the Requested Participant.

C. Each Participant should oppose, to the fullest extent possible consistent with its laws, any application by a third party for disclosure of such confidential information.

D. Notifications and consultations pursuant to Paragraphs II and III of this Memorandum and other communications between or among the Participants in relation thereto should be deemed to be confidential, unless otherwise decided by the Participants.

E. Nothing in this Memorandum prevents disclosure to third parties if such disclosure is required by the law of the Requesting Participant. The Requesting Participant should use its best efforts to notify the Requested Participant at least ten days in advance of any such proposed disclosure, or, if such notice cannot be given, then as promptly as possible.

VI: Changes in Commercial Email Laws

In the event of a significant modification to a Participant's Commercial Email Laws, the Participants should use their best efforts to consult promptly, and, if possible, prior to the entry into force of such enactments, to determine whether this Memorandum should be amended.

VII: Return of Evidence

The Requesting Participant should use its best efforts to keep Evidence shared until the conclusion of the investigation or proceeding specified in the Request and should use its best efforts to return such Evidence at that time if the Requested Participant makes a written request for the retention and return of such Evidence at the time the Evidence is shared.

VIII: Costs

Unless otherwise decided by the Participants, the Requested Participant should pay all costs of executing a Request. When the costs of providing or obtaining information under this Memorandum are substantial, the Requested Participant may require the Requesting Participant to undertake to pay those costs as a condition of proceeding with the Request. In such an event the relevant Participants intend to consult on the issue at the request of either Participant.

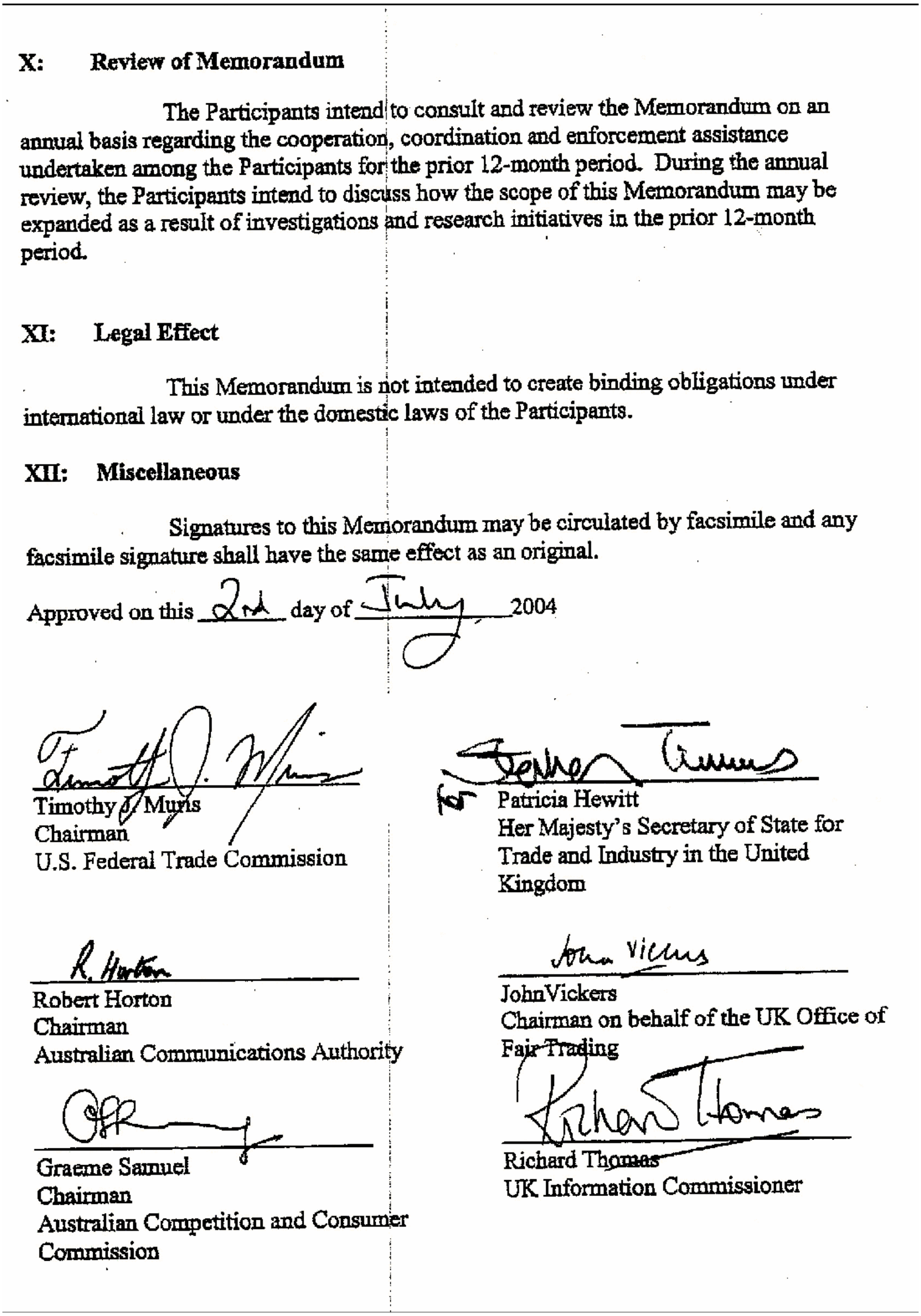
IX: Duration of Cooperation

A. This Memorandum will come into effect on the date that the final Participant to sign this Memorandum executes a signature.

B. Assistance under this Memorandum should be available in investigations or proceedings concerning Spam Violations occurring before as well as after this Memorandum takes effect.

C. A Participant should endeavor to provide the other Participants with 30 days' written notice before ending its cooperation under this Memorandum. However, prior to ending this Memorandum, a Participant should use its best efforts to consult with the other Participants.

D. On cessation of this Memorandum, the Participants should use their best efforts, in accordance with Paragraph V, to maintain the confidentiality of any Request and Evidence communicated to them in confidence by the other Participants under this Memorandum prior to its termination; and to return, in accordance with the provisions of Paragraph VII, any Evidence obtained from the other Participants under this Memorandum.



## X: Review of Memorandum

The Participants intend to consult and review the Memorandum on an annual basis regarding the cooperation, coordination and enforcement assistance undertaken among the Participants for the prior 12-month period. During the annual review, the Participants intend to discuss how the scope of this Memorandum may be expanded as a result of investigations and research initiatives in the prior 12-month period.

## XI: Legal Effect

This Memorandum is not intended to create binding obligations under international law or under the domestic laws of the Participants.

## XII: Miscellaneous

Signatures to this Memorandum may be circulated by facsimile and any facsimile signature shall have the same effect as an original.

Approved on this 2nd day of July 2004

Timothy J. Muris
Chairman
U.S. Federal Trade Commission

R. Horton

Robert Horton
Chairman
Australian Communications Authority

Graeme Samuel
Chairman
Australian Competition and Consumer Commission

for Patricia Hewitt
Her Majesty's Secretary of State for Trade and Industry in the United Kingdom

John Vickers

JohnVickers
Chairman on behalf of the UK Office of Fair Trading

Richard Thomas

Richard Thomas
UK Information Commissioner

## SEOUL-MELBOURNE MULTILATERAL MEMORANDUM OF UNDERSTANDING ON COOPERATION IN COUNTERING SPAM

The Signatories to this Memorandum of Understanding,

CONSIDERING that the protection of the information economy is a major factor for social, economic and environmental development and for the realisation of productivity and service delivery improvements in the government, business and community sectors of each country/region; and

CONSIDERING ALSO that spam can impair the infrastructure and viability of the information economy;

RECOGNISING the necessity for mutual cooperation for the minimisation of spam originating in and being sent to, or by way of, each country/region;

RECOGNISING ALSO that other organisations may in the future wish to be part of this Memorandum and to jointly combat the spam problem;

HOPING to work together to develop cooperative mechanisms to combat the spam problem, including technical, educational and policy solutions; and

DESIRING to enhance cooperative relations,

HAVE REACHED the following understandings:

### Focus of Cooperation

1. Acting within the framework of their powers, interests and responsibilities, the Signatories will collaborate on countering spam (unsolicited commercial electronic messages).

2. The purpose of this Memorandum is to encourage closer cooperation among the Signatories in minimising spam originating in each country/region, passing through each country/region and being sent to end-users in each country/region. The Signatories will also encourage the exchange of information on technical, educational and policy solutions to the spam problem in accordance with the relevant laws and regulations of each country/region and on the basis of equality, reciprocity and mutual benefit.

### Scope of Cooperation

3. The Signatories will promote cooperation in all spheres of activity defined by this Memorandum in order to derive maximum benefits for each and all Signatories.

4. Recognising that bilateral and multilateral cooperation can complement areas of mutual interest in reducing the spam problem, the Signatories have identified areas of common interest for cooperation including, but not limited to, the encouragement of:

a. the exchange of information about policies and strategies for establishing and enforcing anti-spam regulatory frameworks;
b. the exchange of information relating to technical and educational solutions to the spam problem;
c. the exchange of information and strategies about the effective use of regulation policies and in support of enforcement;
d. the exchange of intelligence, relating to the other countries/regions, gathered as a result of enforcement; and
e. industry collaboration.

**Forms of Cooperation**

5. Cooperation among Signatories in the field of countering spam may take the following forms:

a. establishment of channels for exchange of exchange of information on spam, anti-spam measures and emerging issues;
b. exchange of delegations and visits as appropriate;
c. encouragement of liaison between industry and Government organisations to promote areas of interest and cooperation; and
d. other forms of cooperation arranged bilaterally or multilaterally by the Signatories.

**Designated Representative**

6. In order to coordinate cooperative activities, each Signatory will appoint a representative who will act as a contact point, and who will be responsible for determining the particular directions of cooperation and for ensuring the effectiveness of all cooperative activities.

7. The representatives of the Signatories will consult with each other through the channel specified by the Signatories, to define activities and other related matters.

**Activities subject to the Laws of the Signatories**

8. All activities implemented pursuant to this Memorandum will be subject to the respective international obligations and domestic laws and regulations of the Signatories cooperating on any issue.

**Changes in Anti-Spam Legislation and Signing of Other Agreements**

9. In the event of a significant modification to a Signatory's anti-spam legislation, that Signatory will use their best efforts to consult with the other Signatories promptly, either directly or through the Secretary of Signatories as to whether these modifications may have implications for the operation of this Memorandum, and whether the Memorandum should be amended.

10. In the event of a Signatory considering becoming a party to another Agreement that may have implications for the operation of this Memorandum, the Signatory will use their best efforts to consult with the other Signatories promptly, either directly or through the Secretary of Signatories.

**Funding and Resources**

11. The cooperative activities carried out under this Memorandum will be subject to the availability of funds and resources of the Signatories. For those activities carried out under this Memorandum, unless otherwise jointly decided, each Signatory will provide resources adequate to carry out its own commitments in relation to those activities.

**Treatment of "In Confidence" Material**

12. No Signatory will disclose or distribute any information that is supplied and marked, or stated to be 'in-Confidence' by the originating Signatory, except as, and to the extent authorised, by the originating Signatory, or as required by law.

**Settlement of Disputes**

13. Any disputes between any Signatories arising from the interpretation or implementation of this Memorandum will be settled amicably through consultations between the affected Signatories. Should the dispute be of a kind that might warrant a revision of this Memorandum, the parties should advise the Secretary of Signatories so that the matter may be circulated to all Signatories for comment and consideration.

**Secretary of Signatories**

14. The Secretary of Signatories will be an officer of one of the Signatories and will be rotated subject to the agreement of the Signatories. The role of the Secretary will be to act as a contact point for joining this Memorandum and to inform the other Signatories when a new Signatory joins. When a new Signatory joins, the Secretary will include the name of the new Signatory on the List of Signatories at Annex B and advise the contact points of all other Signatories. Contact details for the current
Secretary of Signatories and a description of the role are at Annex A.

**Joining of New Signatories**

15. Participation in this Memorandum is voluntary and is open to the relevant Government and industry organisations of any country/region. All Signatories have equal status.

16. New Signatories will become party to this Memorandum upon acceptance of their credentials by a majority of current signatories, and will signify their intention to participate by completing the details of the Signatory schedule and sending the schedule by facsimile or similar unalterable form to the Secretary of Signatories.
Current signatories to this Memorandum are listed at Annex B.

17. Where more than one Government regulator or industry organisation within one particular country/region is a Signatory to this Memorandum, those regulators and industry organisations will each nominate a single contact point for the purpose of correspondence with the Secretary of Signatories (i.e. where there are two or more government organisations in the same region, they will nominate a single government contact point; where there are two or more industry organisations within the same region they will nominate a single industry contact point).

**Duration of Participation**

18. Each Signatory's participation in this Memorandum will come into effect on the date of signature by that Signatory. It will remain in effect for a period of five (5) years thereafter unless terminated by the Signatory giving six (6) months prior notice in writing to the other Signatories.

19. Not withstanding termination of participation in this Memorandum by any Signatory pursuant to paragraph 18, activities being undertaken pursuant to this Memorandum immediately before its termination will continue to be governed by this Memorandum until their completion, unless the Signatories that are party to the activity mutually determine otherwise.

**Miscellaneous**

20. This Memorandum may be amended or extended at any time by written mutual determination of the Signatories. To this end, signatures to any amendment or extension to this Memorandum may be circulated by facsimile, and any facsimile signature shall have the same effect as an original.