



Anti-Spam Action Plan for Mauritius
(Final Version)

April 2006

National Computer Board

Confidential

Table of Contents

EXECUTIVE SUMMARY	2
1 INTRODUCTION	5
2 ANTI-SPAM COMMITTEE	5
3 THE PROBLEM OF SPAMMING.....	6
4 WHY MAURITIUS NEEDS TO BE PREPARED.....	10
5 APPROACH	11
6 RECOMMENDATIONS	13
6.1 General Awareness for Users and Businesses	13
6.2 Guidelines for ISPs and Other Commercial Organisations.....	16
6.3 Anti-Spam Legislation	18
6.4 International Co-operation.....	21
6.5 Monitoring the action plan	22
APPENDIX 1: RECOMMENDED BEST PRACTICES FOR INTERNET SERVICE PROVIDERS AND NETWORK OPERATORS.....	23
APPENDIX 2: REVIEW OF ANTI-SPAM LEGISLATION IN OTHER COUNTRIES.....	24
APPENDIX 3: AN INTERNATIONAL COMPARISON OF SPAM CONTROL LEGISLATION.....	41
APPENDIX 4: KEY TIPS FOR USERS	45
APPENDIX 5: E-MAIL MARKETING BEST PRACTICE.....	48
APPENDIX 6: LONDON ACTION PLAN	54
APPENDIX 7: ANTI-SPAM ACTION PLAN.....	58
ACRONYMS.....	62

EXECUTIVE SUMMARY

Unsolicited bulk mail volumes now account for as much as one-half of all e-mail traffic on the Internet¹. The main problem with spam and the reason for its proliferation is the shifting of the costs involved away from the advertiser onto the consumer and other parties. Unlike other forms of advertising such as television commercials or billboards, direct marketing usually involves some degree of effort or involvement on the part of the consumer. In most forms of communication, the sender experiences significant and usually measurable costs. Therefore, the sender usually has an incentive to compare the expected benefits of the communication against these costs in deciding whether to proceed with the communication. Email and the Internet change the entire equation because the cost of sending spam is negligible.

Spam is more than a growing nuisance. It is a public policy issue that challenges governments, Internet service providers (ISPs), service providers, marketing agencies and consumers to work together in new ways to solve a problem that threatens the interests of all. Spam also provides a vehicle for activities that are clearly illegal. Such activities include:

- Promoting illegal or offensive content;
- Sending of e-mails with intent to cause fraud and deceit, for example the Nigerian scam and phishing e-mails;
- Sending of malicious software (e.g. spyware, viruses, botnets and Trojan horses); and
- Making unauthorized use of an innocent third party's e-mail server or computer (i.e. zombie) and disguising the e-mail address of the sender to send the e-mails.

To fight spam, governments and companies are looking at a number of possible solutions, including legal and technological safeguards and arrangements to ensure consumers would have a choice in stating whether or not they wish to receive e-mail from a specified sender. However, legal approaches alone are not the right solution. Given the significant rate of increase of spam, it seems reasonable to conclude that current legislative and private responses are having little effect on the activities of most spammers. There is no 'silver bullet' that will eliminate spam entirely however, the incidence of spam can be reduced and controlled. In general, there is a common convergence among most countries that the most effective solution to spam will combine legal, industry self-regulation, public awareness and international co-operation elements.

In Mauritius, the spamming problem is gaining in magnitude² and there is a need to have a concerted approach to address this issue. Without remedial action to address the problem of spam in Mauritius, the country runs the risk of being seen as a safe haven for spammers and there is the risk that legitimate email traffic from Mauritius to other countries which have anti-spam legislation, could be blocked. In this context, the National Computer Board has set up a

¹ Source : Spam Issues In Developing Countries, OECD, DSTI/ CP/ ICCP/ Spam (2005)6/ Final

² Source : State Of Spamming In Mauritius, NCB (2005)

National Anti Spam Committee to co-ordinate activities at the national level with regards to combating spam.

One of the deliberations among members of the Anti-Spam Committee refers to the definition of spam. It was widely acknowledged within the committee that we should have a definition which encompasses the main characteristics of emails falling under the definition of spam.

As such, the spam definition that we have come up with states that *“Unsolicited communications sent in bulk over an electronic media such as e-mail, mobile (SMS, MMS) and instant messaging services, usually with the objective of marketing products or services.”*

Furthermore, after much discussions about the activities which should be run to combat spam at the national level and after taking consideration developments at the level of the ITU³ and other countries such as Canada⁴ and Australia, the Committee came to the conclusion that the recommendations proposed in the Anti-Spam Action Plan will be based around the four main aspects listed below:

- A. General Awareness for users and businesses
- B. Guidelines and Best Practices For ISPs and Other Commercial Organisations
- C. Anti-Spam Legislation
- D. International Co-operation

The main recommendations and proposed actions for each of the above are shown below:

A. General Awareness for users and businesses

Recommendation 1: Public Awareness Campaign

Recommendation 2: Best Practices for IT Professionals

Recommendation 3: Monitor Effectiveness of the Awareness Campaign

B. Guidelines and Best Practices for ISPs and Other Commercial Organisations

Recommendation 4: Adoption of Industry Best Practice Guidelines by ISPs and Network Operators

Recommendation 5: Best Practices for E-Mail Marketing

Recommendation 6: ISPs and service providers to implement measures to prohibit spamming activities on their networks

Recommendation 7: Guidelines to limit the problem of open relays

C. Anti-Spam Legislation

Recommendation 8: Review of legal framework and drafting of Anti-Spam legislation for Mauritius

³ See ITU Anti-Spam website at <http://www.itu.int/osg/spu/spam>

⁴ See Canada Anti-Spam Action Plan at http://e-com.ic.gc.ca/epic/Internet/inecic-ceac.nsf/en/h_qv00246e.html.

D. International Co-operation

Recommendation 9: Participation in multilateral and bilateral initiatives

Recommendation 10: International Co-operation with ITU and African ISP Association

E. Leadership and Monitoring of Action Plan

Recommendation 11: Setting up of a central co-ordination body at the NCB to monitor and review the implementation of the proposed action plan and recommend future actions.

The detailed action plan for the recommendations can be found at Appendix 7⁵ of the report.

⁵ Page. 62

1 INTRODUCTION

Spam is generally defined as unsolicited electronic messages usually sent in bulk for commercial purposes via email. Spam largely takes the form of unwanted, unsolicited, emails via the internet which are usually sent to promote goods and services or scam. It can also include other forms of electronic messages such as text messages using Short Message Service or Multimedia Message Service.

Spam does not refer to legitimate commercial email for which the recipients have given their consent. Spam is often a source of scams, viruses and offensive content. Spam is a major problem that takes up valuable time and increases costs for consumers, business and governments.

In line with the mission of the National Computer Board (NCB) to promote the development of the ICT Sector, the Board had taken the initiative to develop an Anti-Spam action plan for Mauritius to address the issue of spamming. In this context, an Anti-Spam committee was set up.

This report describes the scope of the problem of spamming in the world, why Mauritius has to be prepared to fight it and the recommendations of the Anti-Spam Committee for tackling the problem of spamming.

2 ANTI-SPAM COMMITTEE

The terms and reference of the Anti-Spam Committee are to:

- develop a National Anti-Spam Action Plan for Mauritius;
- make recommendations on public awareness programmes to educate the public and businesses on the steps that they can take to protect themselves from spam;
- review the current legal framework and make recommendations on legislative proposals for spamming;
- develop anti-spam guidelines to be adopted by the local ISPs and codes of practice for industry players; and
- recommend measures at the international level to counter spamming.

The composition of the committee is as follows:

- Mr K. Mohee, Executive Director, NCB (Chairman)
- Mr V. Mauree, Manager – Planning, Research and Development, NCB

- Mr S. Bissessur, Project Manager – IT Security Unit, Ministry of IT and Telecommunications
- Mr R. Makoond, Executive Director, Joint Economic Council
- Mr T. Dabeesing, IT Manager, ICT Authority
- Mr M. Oozeer, Ag. Senior State Counsel, Ministry of Justice and Human Rights
- Dr. V. Padayatchy, Secretary, ACT
- Mr N. Le Maire, Representative of MITIA
- Mr J.Lim Fook, Networks & Systems Manager, Telecom Plus Ltd
- Mr N.Maudarbocus, IT Lecturer, Mauritius Chamber of Commerce & Industry
- Mr D. Babooa, Business Analyst, NCB (Secretary)

3 THE PROBLEM OF SPAMMING

Spam directly engages a very wide range of stakeholders that includes individual consumers, all organizations of whatever size in the private and public sectors that are Internet users, network operators and Internet Service Providers (ISPs), suppliers of Internet security products and services, commercial e-mail marketers, entities and organizations that commission spamming campaigns, a variety of government policy departments, regulatory authorities and enforcement agencies at the national level, and various intergovernmental and other international organizations at the regional and global levels.

Given the range of stakeholders engaged in the debate about spam and the diversity of their interests, it is perhaps not surprising that there is not at present an international consensus on the definition of spam, the specific governance issues it raises, or the most appropriate methods of resolving these issues.

Although there is not at present an international consensus on the definition of spam, there is a fairly widespread agreement that spam exhibits certain general characteristics⁶:

- Firstly, spam is an electronic message. For most purposes, this may be restricted to email, but other methods of delivering spam do exist, including the Short Messaging Service, or SMS, Voice over IP, mobile phone multimedia messaging services, instant messaging services.

⁶ ITU Survey on Anti-Spam Legislation Worldwide, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June – 1 July 2005

- Secondly, spam is unsolicited. 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.
- Thirdly, 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).

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.”⁷

In general spam messages tend to fall into the following categories:-

- Unsolicited commercial advertising;
- Pornography;
- Scams or fraud;
- Propaganda; and
- Chain letters.

Some stakeholders define spam broadly to include all unsolicited bulk commercial e-mail sent for direct marketing purposes or, more colloquially, as ‘electronic junk mail’. By this broad definition it is estimated that considerably more than half the e-mail sent today is spam. Other stakeholders define spam more narrowly as commercial e-mails that are fraudulent, malicious, or misleading. In many cases, such e-mails violate national laws. Although it was originally confined to e-mail services and directed at consumers and users that used wired technologies to access the Internet, spam is now spreading to other kinds of networks and services, including cellular telephone networks, weblogs, and instant messaging services in both wired and wireless environments (where it is known as ‘spim’).

⁷ ITU Survey on Anti-Spam Legislation Worldwide, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June – 1 July 2005

Following discussions among members of the Anti-Spam Committee with regard to the definition of spam, it was widely acknowledged within the committee that we should have a definition which encompasses the main characteristics of emails falling under the definition of spam.

As such, the spam definition that we have come up with states that *“Unsolicited communications sent in bulk over an electronic media such as e-mail, mobile (SMS, MMS) and instant messaging services, usually with the objective of marketing products or services.”*

Although wireless spam and spim raise somewhat different issues from conventional spam, because of differences that typically exist in the design, operation, regulation and tariffing of services on these different kinds of networks, spam raises similar general concerns in all network and service environments.

From this broad perspective, spam raises a number of different kinds of governance issues.

- Spam can be annoying or offensive to consumers and imposes various additional costs, especially on individuals who access the network through pay-per-use or low bandwidth connections, thereby hampering the development of Internet access.
- Spam imposes significant costs on organizations in the private, public and not-for-profit sectors, whose employees may spend substantial amounts of work time sorting through email messages to determine which are legitimately related to their work, and in deleting the rest.
- Spam also imposes significant costs on Internet Service Providers (ISPs) and other network operators, since it requires investment in a range of tools that are needed to counter spam, including anti-spam technologies (e.g. filtering technologies), server and transmission capacity, human resources, and anti-spam information sharing, cooperation, and regulatory structures. This is a particularly important concern in developing countries.
- Spam provides a cover for spreading viruses, worms, trojans, spyware, etc., which typically are sent as attachments to e-mail messages, which may cause harm to individual consumers and user organizations, as well as to network operators and service providers.
- As well causing inconvenience and reducing the utility of the Internet for consumers and users, spam may violate national law – e.g. if it constitutes an invasion of privacy (e.g. spyware), leads to malicious attacks on their personal property (e.g. viruses), or

results in the unauthorized use of this property, possibly for illegal purposes (e.g. zombie networks).

- Spam also provides a cover for other forms of cyber crime, such as identity theft through “phishing” and other forms of online fraud, which cause harm to individual consumers and impose costs on corporations (e.g. in the financial services sector), and government agencies (e.g. that issue licences).

At the WSIS thematic meeting on Countering Spam held in July 2004, ITU mentioned that “unsolicited commercial communications” or so-called spam has grown into one of the major plagues affecting today's digital world. As much as 80% of all e-mail traffic is spam, compared to 35% a year ago, with spammers sending hundreds of millions of messages per day. The estimated costs of spam to the global economy are approximately US\$25 billion dollars per year. The problem is spreading also to cell phones. In Japan, nine out of ten junk e-mails come in the form of mobile telephone text messages.

For all these reasons, there is growing concern that if spam is not controlled, it will constitute a serious impediment to Internet use for consumers and users, and a significant roadblock to the development of e-commerce, e-government, and online public services, thereby reducing the “social value” of the Internet. This is of particular concern to government policy-makers in developed and developing countries, although the specific concerns it presents may vary according to the level of technological and economic development within a country.

At the same time, it is also generally recognized that commercial e-mail, which does not raise the kinds of issues listed above, has a legitimate place in the development of e-commerce and the e-economy, and that measures to control spam must distinguish between acceptable and unacceptable commercial e-mail practices. This is of particular concern to businesses in both developed and developing countries, which see the new commercial opportunities made possible by e-mail and want to avoid being subjected to overly onerous laws and regulations.

In this regard, commercial e-mail may be seen as a ‘two-edged sword’ by small and medium sized enterprises (SMEs) in developing countries. On the one hand, it offers an opportunity to market their products and services internationally, and to participate in global e-commerce. On the other hand, the anti-spam laws and regulations being developed and implemented in other countries may create uncertainty and add to the cost and complexity of business operations.

The intrusiveness of spam, much of it linked to fraudulent, deceptive or pornographic commercial activities and increasingly carrying computer viruses, has raised questions about the future development not only of e-commerce and e-mail marketing but also of e-government.

4 WHY MAURITIUS NEEDS TO BE PREPARED

The problem of spamming is becoming more and more prevalent in Mauritius as well. There is not much information available currently as to the extent of the problem in Mauritius. According to Telecom Plus Ltd, one of the internet service providers in Mauritius, about 65% of e-mail messages received at their level are spam. Most of the spams originate from overseas. In most cases the spammers hide their e-mail address or use spoofing techniques so that it becomes difficult for the recipient to identify the sender.

It has also been observed by NCB that there is not a concerted approach at the level of ISPs to tackle the problem yet. For example, not all ISPs offer an anti-spam service. It has been observed by Telecom Plus Ltd that the common means which are being adopted by spammers targeting local servers in Mauritius are as follows:

- E-Mail harvesting
- Open relays
- Zombies

The spamming problem must not be underestimated as it could represent a major obstacle to the development of the ICT sector. Most of the spam e-mails that are received in Mauritius originate from overseas. Any one in Mauritius can become a victim of spam. In addition, phishing and identity theft represent the most dangerous forms of electronic fraud that can happen via spam. Spammers often form part of an international network of crime and it is necessary to have a co-ordination at the international level as well on this issue. Spamming is a form of Internet crime and has to be addressed as such.

In addition to imposing a cost burden, spam is now undermining the reliability of e-mail networks for business users. It also threatens consumer confidence in the new e-commerce marketplace. Because of this, the potential of information and communications technology to improve productivity is now being threatened by spam. If Mauritius is to become a Cyber Island and ICT sector the fifth pillar of our economy then we have to address the spamming problem.

The consequences of spam for businesses in Mauritius can be quite costly if nothing is done to educate users about the problem, to seek the support of ISPs and industry players in implementing anti-spam measures and to come up with appropriate legislative measures to combat the problem.

5 APPROACH

The NCB had prepared a preliminary report⁸ to assess what was being done at the international level in order to tackle the spamming problem in other countries and also at the level of ITU. This report was used as basis for discussion at the level of the Anti-Spam Committee.

A paper on the current situation of the spamming problem in Mauritius was prepared following the first meeting of the committee. Members of the committee were invited to submit their views on the problem and to propose solutions for tackling the problem.

During discussions, it was noted that most anti-spam initiatives aimed at controlling the growing volume of unsolicited commercial email focused on a combination of filtering technologies and the use of “black lists” of servers and domains that have been identified as sources of spam. As these spam-control services have become more and more sophisticated, so have the tactics used by spammers to bypass them.

However, these technical solutions have certain drawbacks. Legitimate commercial email communications, as well as legitimate non-commercial and personal email communications, can be blocked by filters, sometimes without the knowledge of either the senders or the intended recipients. These filtering techniques and practices, though well intended, can contribute to undermining consumer confidence in the reliability of email.

It was therefore noted that such techniques, such as black lists and filtering are not silver bullets that will solve all the issues related to spam. In addition to these technical solutions, there are a range of best practices and guidelines that can be adhered to by commercial e-mail senders to reduce the spam-related threats to the Internet. The main challenge is to identify and implement a winning combination of sound business practices and effective technical solutions.

There was a general agreement on the following kinds of factors can be used to distinguish between acceptable and unacceptable commercial e-mail practices:

- consumer and user consent;
- e-mail intent;
- mechanisms for authorizing or certifying information sources;
- honesty and transparency of communications;
- mechanisms for receiving and redressing consumer complaints; and
- mechanisms to permit e-mail recipients to opt-out of receiving future communications.

⁸ The Problem of Spamming (2005)

Following discussions and after taking consideration developments at the level of the ITU⁹ and other countries such as Canada¹⁰ and Australia, the Committee came to the conclusion that the recommendations proposed in the Anti-Spam Action Plan will be based around the four main aspects listed below:

- General Awareness for users and businesses
- Guidelines For ISPs and Other Commercial Organisations
- Anti-Spam Legislation
- International Co-operation

The actions recommended for each of the above are elaborated in the next section. The detailed action plan is at Appendix 7¹¹.

⁹ See ITU Anti-Spam website at <http://www.itu.int/osg/spu/spam>

¹⁰ See Canada Anti-Spam Action Plan at http://e-com.ic.gc.ca/epic/Internet/inecic-ceac.nsf/en/h_gv00246e.html.

¹¹ Page 62

6 RECOMMENDATIONS

6.1 General Awareness for Users and Businesses

While there is much that law enforcement agencies, ISPs and other network operators, and businesses can do to fight spam, there is a general agreement that all Internet end-users, whether they are employees, students or consumers, have an important role to play in fighting spam.

It is also clear that, in order to help Internet users play their part, more needs to be done to inform them about what they can do to limit the amount of unwanted commercial email they receive, to protect themselves and others against viruses, to avoid falling prey to fraud and to prevent their computers from being turned into zombies used without the user's knowledge to send spam.

There is a considerable amount of readily available information on the steps users can take to limit the amount of spam they receive and avoid falling victim to the kinds of deceptive, fraudulent or other criminal practices associated with spam. However, more effort is needed to communicate this information, particularly as it pertains to emerging threats.

The National Computer Board will be taking the lead in co-ordinating the implementation of the different actions for this element of the strategy.

RECOMMENDATION 1: PUBLIC AWARENESS CAMPAIGN

The Committee recommends that a multi-stakeholder public awareness campaign be initiated with the involvement of ISPs, consumer groups, private sector and government to educate users on how to protect themselves against spam.

Specific actions to be implemented in this respect:

1. *Anti-Spam Day: 1st June*

It is recommended that an Anti-Spam Day be set on the 1st June of each year. This will help in attracting the marketing of the activities for the awareness campaign and can be used to kick-start the activities for the Anti-Spam initiative.

2. *Common Anti-Spam Slogan*

The recommended slogan is as shown in the next page.

STOP SPAM!

Spam is commonly referred as unsolicited communications sent in bulk over an electronic media such as e-mail, mobile (SMS, MMS) and instant messaging services, usually with the objective of marketing products or services.

Key Tips for Users

1. Protect your computer

Spam is a growing source of computer viruses. It is critical that you protect your computer from virus-carrying messages. Install and regularly update antivirus and anti-spam software. If you don't have the extra protection of a firewall, get it.

2. Protect your email address

Reserve one email for your trusted personal and business contacts. Create a separate, expendable email address for other online uses.

3. Protect yourself

Don't try, don't buy and don't reply to spam. Just delete it. It's a great way to prevent receiving more spam in the future. Opt out from the sender's mailing list if given the option. Configure your email client (e.g. Outlook) so as to block incoming mail from spammers.

Critical to this initiative is the development of consistent simple messages and a common look for the slogan, and the broad dissemination, by a wide range of partners. It is proposed that a similar slogan as adopted by Canada, which is based on three key tips to help users protect themselves and fight spam, be adopted for Mauritius. The slogan will be disseminated to different stakeholders to be published on their websites and in the media.

3. *Anti-Spam Awareness Sessions for students and general public*

The National Computer Board will provide anti-spam awareness sessions for the general public and students through the ICT Literacy Programme of the IT Coaches and would sensitise students in schools on the spamming problem through seminars during the Internet Fiesta event.

Other organisations such as the Internet Child Safety Foundation and Internet Society would be encouraged to participate in the anti-spam education campaign. It is therefore proposed that the NCB would organize a high level workshop each year with regards to disseminating information and best practices for end users with regards to fighting spam.

4. *Anti-Spam Awareness Sessions for workers*

All stakeholders will be invited to provide anti-spam awareness sessions for their employees. The NCB will work with the IT Security Unit, Ministry of IT and Telecommunications to sensitise employees in the public sector on the problem of spamming and preventive measures that need to be adopted in order not to fall victim to spam.

5. *Anti-Spam Awareness Programme on TV*

A 10-15 minute video footage illustrating the problem of spamming and measures that users should adopt would be realized by the NCB with the support of the Ministry of IT and Telecommunications, ACT, Mauritius IT Industry Association, MBC, ISPs and ICT Authority. The video will be subsequently aired on TV.

6. *Setting up of Anti-Spam Website*

The National Computer Board with the partnership of ISPs, ACT and MITIA will set up an anti-spam website to provide information about anti-spamming measures and guidelines, anti-spam legislation, facilities to report spam and latest developments in spamming for different audiences, such as general public, students, SMEs and IT professionals.

7. *Publication and Dissemination of anti-spam brochures and guidelines*

The NCB will publish and disseminate anti-spam brochures and guidelines after consultation with all stakeholders. Because of their direct relationship with Internet users, ISPs are in good positions to deliver a public education and awareness campaign in partnership with consumer groups and governments. In this respect, it is recommended that:

- a) ISPs include regular information about anti-spam measures for their customers when issuing their invoices; and
- b) The NCB together with ICT Authority, ACT, Mauritius Chamber of Commerce and Industry and Mauritius IT Industry Association will work out a brochure and guide for consumers to educate people about the problem and what measures they can implement in order not fall victim to spam. An example of general information on tips for users regarding spam that can be included in the brochure and guide is at Appendix 3.

8. *Inclusion of Spam Information in IT Curriculum.*

The Ministry of Education and Human Resources will be invited to include in the IT Curriculum at the secondary level, information about what is spamming and what measures students need to be aware of in relation to it.

RECOMMENDATION 2: BEST PRACTICES FOR IT PROFESSIONALS

1. *Organisation of technical workshops*

The NCB with the support of IT Security Unit – Ministry of IT and Telecommunications, ICT Authority, ACT and MITIA will organize two technical workshops each year for IT professionals to disseminate best practice information on protecting e-mail servers against spam and other anti-spam related technology solutions.

RECOMMENDATION 3: MONITOR EFFECTIVENESS OF AWARENESS CAMPAIGN

The following action is recommended:

1. *Annual Spam Study*

The NCB with the support of ICT Authority, ACT and MITIA would carry out two studies on an annual basis to assess awareness of users about the spam problem and the effectiveness of the measures that have been implemented. One study would be targeted towards end users and the other would be targeted at the level of businesses.

6.2 Guidelines for ISPs and Other Commercial Organisations

Any measure aimed at successfully protecting the security of Internet communications from threats such as spam, viruses and spyware must involve the co-operation of the government and other stakeholders concerned. By its underlying architecture, the Internet is an open network of networks that allows the free flow of information.

There are, however, a number of known practices that permit spam and other forms of network abuse to happen. These include leaving servers open to relay and forward messages, thereby allowing computer systems to be hijacked as proxy email servers for abusers.

While the problem of spam, like the Internet itself, is global in scope, network-management actions taken in Mauritius can contribute to the solution. Those who own and manage networks and facilities must adopt best practices that will effectively reduce and control spam and related threats.

Industry stakeholders have the responsibility to agree on basic operating practices for network facilities that will reduce spam, and show commitment to reduce spam by requiring the adoption of these practices on networks and facilities based in the country.

RECOMMENDATION 4: INDUSTRY BEST PRACTICE GUIDELINES FOR ISPS AND SERVICE PROVIDERS

The Committee recommends that ISPs and service providers under the ICT Act 2001 adhere to the best practices mentioned in Appendix 1. This will help reduce spam and related threats.

The objectives of the Best Practices are to:

- (a) Provide guidelines for ISPs and Service Providers to promote the adoption of responsible processes and procedures for dealing with Spam;
- (b) Ensure these guidelines are developed in such a way as to achieve a balance between legitimate industry interests and viability and user interests; and
- (c) Promote end user confidence in and encourage the use of the Internet.

In seeking to achieve its objectives the following principles have been adhered to:

- (a) Ensure there is a balance between legitimate industry interests and viability and End User interests;
- (b) Any rules should not adversely affect the commercial viability of ISPs and Service Providers and the services they make available.
- (c) Spam is an inherent risk when using the Internet and as such ISPs and Service Providers and Users alike have an obligation and duty to implement measures to attempt to minimise the Spam burden.

The recommendations for best industry practices are voluntary and the actual timeframes may vary, depending on the particular operator's network and business. In some cases, alternative solutions may lead to the same objectives as mentioned in the recommendations. In this respect and because of the rapid changes in technology, it is recommended that the best practices should not be treated as mandatory requirements.

It is recommended that a working group be set up to make recommendations for future actions regarding best practices to be adopted by ISPs.

RECOMMENDATION 5: BEST PRACTICES FOR E-MAIL MARKETING

Organisations are recommended to adopt the best practices mentioned at Appendix 4 as a way to ensure that their own legitimate messages are not blocked by anti-spam technology implemented by ISPs and other operators. The Code of Practice at Appendix 4 has been

based on the Canadian Model¹² of recommended best practices for email marketing. The best practices are not legally binding but are intended to complement other laws that govern privacy and electronic transactions such as the Data Protection Act 2004, ICT Act 2001, Electronic Transactions Act 2000 and Computer Misuse and Cybercrime Act 2003.

The effectiveness of these practices should be reviewed on an ongoing basis. It is recommended that a working group be set up to address this issue and make recommendations for future actions.

RECOMMENDATION 6: ISPS AND SERVICE PROVIDERS TO PROHIBIT SPAMMING ACTIVITIES ON THEIR NETWORKS

ISPs and service providers should adopt and enforce Acceptable Use Policies (AUPs) that clearly prohibit spamming activities on their networks.

RECOMMENDATION 7: GUIDELINES TO LIMIT PROBLEMS CAUSED BY OPEN RELAYS

It is recommended that ISPs and service providers implement the following measures to reduce the problems caused by open relays:

- ISPs and service providers must restrict inbound connections to any service they manage that allow email forwarding on behalf of third parties. Such restriction must limit access to the service to a closed user group relevant to the use of the application that the service facilitates.
- ISPs and service providers must require, by way of their AUP, the same action from their subscribers to the restrictions mentioned in the above paragraph.
- ISPs and service providers must provide, in their AUP, a clause that allows for immediate account disconnection or suspension when the ISP / service provider becomes aware of inbound connections to any service they host that allows email forwarding on behalf of third parties, regardless of whether the open service is provided intentionally, through wrongly configured, or by other means not authorised by that third party including but not limited to through a Trojan horse or virus.

6.3 Anti-Spam Legislation

The vast majority of spam reaching Mauritian citizens and businesses originates outside Mauritius. However, with a sound legislative framework in place, and with effective investigation and enforcement capabilities, Mauritius would be in a better position to work towards internationally harmonized approaches and cooperative enforcement actions.

¹² Stopping SPAM, Report of the Task Force on Spam, May 2005

One of the first questions facing the Committee was how well the current legal framework measured up to combating the spam problem.

Spamming is not regulated in Mauritius. However, the problem of spamming is, indirectly dealt with under the Data Protection Act (the “**Act**”). When one speaks of ‘spam’, the term is generally used to refer to unsolicited bulk messages, usually transmitted to a large number of recipients via electronic mediums, such as electronic mails. The Act deals with the processing of personal data for direct marketing.¹³

According to the Act, personal data must be collected fairly, for specified purposes, and processed in a fair and lawful manner in line with those stated purposes. The definition of personal data is sufficiently wide to catch the email addresses of living individuals, however those email addresses are reprocessed. Email addresses often contain the user’s name as well as information on the country of residence or the service provider. The definition of processing is sufficiently wide to include the steps that have to be carried out to send emails to people with those addresses.

Under the provisions of the Act, a person may, at any time, request by notice in writing a data controller who holds personal data about him, to stop or not to begin, the processing of such data or information for the purposes of direct marketing.

Whenever a data controller receives such a request he shall, as soon as reasonably practicable and in any event not more than 28 days after the request has been received either erase the data where the data is kept only for the purposes of direct marketing or, stop the processing of the data for direct marketing where the data is kept for direct marketing and other purposes.

Furthermore, the Information and Communication Technologies Act (ICT Act) makes it offence for any person who “uses an information and communication service ... for the purpose of causing annoyance, inconvenience or needless anxiety to any person”.¹⁴

Finally, as regards the misuse of computers to cause denial of service attacks and the transporting of viruses, the Computer Misuse and Cybercrimes Act (the “**CMC Act**”) provides for the offences of ‘unauthorised modification of computer material’¹⁵ and ‘damaging or denying access to computer system’¹⁶.

¹³ s. 30

¹⁴ s. 46 (h)(2) of the ICT Act

¹⁵ s. 6 of the CMC Act

¹⁶ s. 7 of the CMC Act

The Committee also examined legislation approaches in other countries. A review and comparison of the provisions of legislations in other countries can be found at Appendices 2 and 3.

It is the view of the Committee based on the experiences of other countries that there should be a specific Anti-Spam legislation to establish a clear set of rules to prohibit spam and other emerging threats to the safety and security of the Internet (e.g. botnets, spyware, keylogging). Amendments to existing laws may also be required.

RECOMMENDATION 8: REVIEW OF LEGAL FRAMEWORK AND DRAFTING OF ANTI-SPAM LEGISLATION FOR MAURITIUS.

The Committee therefore recommends that a specific legislation be introduced to address the problem of spamming in Mauritius which will have specific provisions for the following spam related actions:

- The use of false or misleading headers or subject lines (i.e. spoofing of e-mails) in order to hide the source (i.e. origin), purpose or contents of an email, whether the objective is to mislead recipients or to evade technological filters;
- Whether to abide by an opt-in/ opt-out or both regime for sending unsolicited commercial email;
- The construction of false or misleading URLs and websites for the purpose of collecting personal information under false pretences or engaging in criminal conduct (or to commit other offences listed) – i.e phishing and pharming;
- The harvesting of email addresses without consent, as well as the supply, use or acquisition of such lists; and
- Dictionary attacks.

It is further recommended that the legislation be technology neutral in order to cater for the different media (whether wireless or wired) through which spam can originate and the proposed legislation may be based on the ITU's draft model legislation on spam¹⁷.

As such a definition of the term spam need not be included in the legislation as is the case in other countries. The term unsolicited communications which is technology neutral can be considered as an alternative means to refer to spam and can be used instead in the legislation.

¹⁷ See www.itu.int/ITU-D/treg/Events/Seminars/2005/GSR05/Documents/GSR_Discussion_Paper_Spam.pdf

6.4 International Co-operation

The combination of technical solutions, user awareness, appropriate and balanced legislation followed up with measured enforcement, industry initiatives including those by the marketing community, and international cooperation, are all indispensable methods which can be used to combat spam.

It has been estimated that a large proportion of the spam received in Mauritius originates from overseas. This reflects the fact that, because of the open nature of the Internet, spam can potentially be sent from anywhere, to anywhere. Stopping spam therefore requires the cooperation among different countries in enforcing anti-spam laws.

RECOMMENDATION 9: PARTICIPATION IN MULTILATERAL AND BILATERAL INITIATIVES

To this end the committee is recommending that Mauritius participate in multilateral and bilateral initiatives on the international front to fight spam.

The main multilateral initiative that can be considered is the London Action Plan (LAP). The London Action Plan was initially launched after a conference on spam enforcement hosted jointly by the UK Office of Fair Trading and the US Federal Trade Commission in London in October 2004. It was the first international forum to focus exclusively on spam enforcement. The result of this meeting was the London Action Plan on International Spam Enforcement Cooperation, which aims to develop ways and means of improving international cooperation in dealing with spam and spam-related problems. The details of the LAP are at Appendix 5.

Since most of the spam originates from overseas, it is also recommended that bilateral agreements with countries like United States and Australia be considered for implementation. The United States and Australia have been very active in this arena and Mauritius could benefit from such co-operation.

RECOMMENDATION 10: INTERNATIONAL COOPERATION WITH ITU AND THE AFRICAN ISP ASSOCIATION

It is recommended that Mauritius participate in international forums on the spamming problem such as:-

- Interaction with ITU Study Group 17 which deals with the spam problem
- Interaction with the ITU Strategy and Policy unit regarding the spam problem
- Contribution to the African ISP Association working group on spam
- Technical training on countering spam via the African Network Operating Group (AFNOG)

6.5 Monitoring the action plan

It is recommended that a central co-ordinating body be assigned the responsibility to monitor the different actions recommended in the action plan and to also carry out further assessments where necessary to recommend future actions to combat spam. The Anti-Spam Action Plan is a dynamic process and there is a need to put in place a proper framework to ensure that there is a proper follow-up on actions recommended and a roadmap for action be established to combat spam.

RECOMMENDATION 11: ANTI-SPAM COMMITTEE

It is therefore recommended that an Anti-Spam Committee be established at the level of the National Computer Board to monitor the implementation of the action plan, act as a platform for stakeholders to share information on best practices to reduce spam and provide policy guidance on measures for future actions to combat spam in Mauritius.

The proposed framework is shown below.

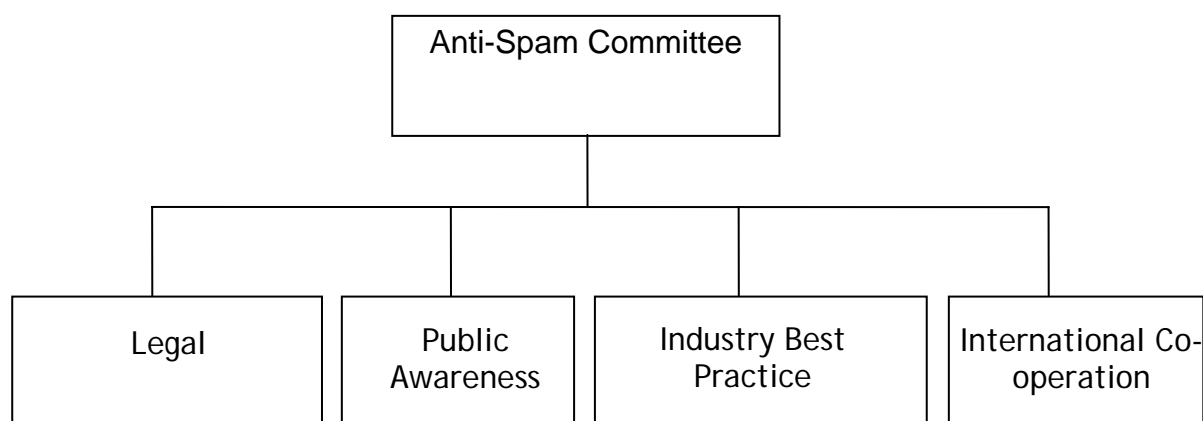


Fig 1: Anti-Spam Committee

It is recommended that four working groups be established under the Anti-Spam Committee to look into the aspects of legal framework, public awareness, industry best practice and international co-operation.

APPENDIX 1: RECOMMENDED BEST PRACTICES FOR INTERNET SERVICE PROVIDERS AND NETWORK OPERATORS

Recommended Best Practices for Internet Service Providers and Other Network Operators (Based on Canada's Anti-Spam Action Plan)

1. All registrants and hosts of domain names should publish Sender Policy Framework (SPF) – addresses of its email servers – information in their respective domain name server zone files as soon as possible.
2. ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive email over port 25 should be restricted to hosts and the provider's network. Use of port 25 by end-users should be permitted only on an as-needed basis, or as set out in the provider's end-user agreement / terms of service.
3. ISPs and other network operators should block email file attachments with specific extensions known to carry infections, or should filter email file attachments based on content properties.
4. ISPs and other network operators should actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and should respond appropriately.
5. ISPs and other network operators should establish and consistently maintain effective and timely processes to allow compromised network elements to be managed and eliminated as sources of spam.
6. ISPs and other network operators should establish appropriate intercompany processes for reacting to other network operators' incident reports.
7. ISPs, other network operators and enterprise email providers should communicate their security policies and procedures to their subscribers.
8. ISPs and other network operators should implement email validation on all their Simple Mail Transfer Protocol (SMTP) servers (inbound, outbound and relay).
9. Non-delivery notices (NDNs) should only be sent for legitimate emails.
10. ISPs and other network operators should 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. This information should include points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address.
11. ISPs and other network operators should 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. All local area network (LAN) operators should be compliant with Request for Comments (RFC) 1918 — "Address Allocation for Private Internets." In particular, LANs should not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.
12. ISPs and other network operators should prohibit the sending of email that contains deceptive or forged headers. Header-tracing information should be correct and compliant with relevant RFCs, including RFC 822 and RFC 2822; and reference domains and IP addresses should have up-to-date, accurate registration information.

APPENDIX 2: REVIEW OF ANTI-SPAM LEGISLATION IN OTHER COUNTRIES

THE UNITED KINGDOM

In the United Kingdom, the Government introduced the Electronic Commerce (EC Directive) Regulations 2002.¹⁸ These required "unsolicited commercial communications" to be clearly identified and identifiable as such, upon receipt. The responsibilities of UK advertisers in relation to email were increased further on June 4, 2003 when the new Sales Promotion and Direct Marketing Code ("the Code") issued by the Committee of Advertising Practice ("CAP")¹⁹ came into force. CAP is the self-regulatory body that creates, revises and enforces the Code. CAP's members include organisations that represent the advertising, sales promotion, direct marketing and media businesses. From the consumer's perspective, the "teeth" of the Code lie in the administration of it that is undertaken by the Advertising Standards Authority.²⁰

The new CAP Code makes the following provisions in relation to spam:

1. Unsolicited email marketing communications must be clearly identifiable as marketing communications without the need to open them up.
2. Any other unsolicited email marketing communications, marketing communications for employment agencies and distance selling communications that require payment before products are received must contain specified information before contacting the seller.
3. The "explicit consent" of consumers is now required before marketing by fax, by email or by way of SMS text transmission, with the sole exception that marketers may market similar products to existing customers.

Finally, on December 11, 2003, a new UK spam law took effect. The new law is in fact a set of regulations, entitled the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "**PEC Regulations**")²¹. These Regulations superseded the Telecommunications (Data Protection and Privacy) Regulations 1999.²² One of the main aims of this Directive was to ensure the "protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector".

¹⁸ See www.hmso.gov.uk/si/si2002/20022013.htm

¹⁹ See www.cap.org.uk

²⁰ See www.asa.org.uk

²¹ (SI 2003/2426)

²² The 1999 Regulations imposed rules on the use of telecommunications services and gave effect to EU Directive 97/66.

Regulation 22 of the PEC Regulations prohibits spam without prior consent unless the exception applies. Regulation 22 provides:

22. Use of electronic mail for direct marketing purposes

22. (1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.

(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where-

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person's similar products and services only;

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

(4) A subscriber shall not permit his line to be used in contravention of paragraph (2).

Regulation 23 of the PEC Regulations provides:

23. *Use of electronic mail for direct marketing purposes where the identity or address of the sender is concealed*

23. A person shall neither transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by means of electronic mail-

(a) where the identity of the person on whose behalf the communication has been sent has been disguised or concealed; or

(b) where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided."

The practical effect of the PEC Regulations upon businesses and consumers in the United Kingdom is described below:

A. For all marketing messages sent by electronic mail, regardless of who the recipient is -

- (i) the sender must not conceal their identity; and
- (ii) The sender must provide a valid address for opt-out requests.

B. For unsolicited marketing messages sent by electronic mail to individual subscribers only, an "opt in" applies. Senders must not send such messages unless they have the recipient's prior consent to do so. The opt-in rule is relaxed if three exemption criteria are satisfied:

- (a) the recipient's email address was collected "in the course of a sale or negotiations for a sale";
- (b) the sender only sends promotional messages relating to their "similar products and services"; and
- (c) when the address was collected, the recipient was given the right to opt out (free of charge except for the cost of transmission) which they did not exercise. The opportunity to opt out must be given with all subsequent messages.

An "individual subscriber" is defined as a residential subscriber, a sole trader or an unincorporated partnership in England, Wales and Northern Ireland. Scottish partnerships were excluded, presumably because they have a separate legal persona distinct from that of the individual partner.

Therefore, after December 11, 2003, it is offence for a "person" (presumably meaning any legal person-the Regulations do not define the term) to send an unsolicited email or SMS text message to a UK consumer unless:

- (a) there is an "existing customer relationship"; or
- (b) they have given their permission to receive the material.

The view of the Department of Trade and Industry (DTI)²³ is that the recipient has to agree in advance to being sent marketing emails, except where there is an existing customer relationship, where companies may continue to email or text for the purposes of marketing their own similar products on an "opt out" basis.

C. "Existing customer relationship"

What is an "existing customer relationship"? First, the sender must have obtained the customer's email address in the course of "the sale or negotiations for the sale of a product or service to the recipient". On the face of it, this would appear to exclude the provision of data

²³ See www.dti.gov.uk/industries/ecomunications/directive_on_privacy_electronic_communications_200258ec.html

during a website registration process. However, the prevailing view of the DTI is that "existing customer relationship" is wide enough to cover such pre-contractual communications.

D. Similar goods and services

Permission to send spam to existing customers is restricted to "similar products and services only". Thus, buying a wardrobe from an online retailer would permit the retailer to email you in relation to white goods, but not banking facilities from a bank. The customer must be given an easy way of suppressing the use of personal data for the purposes of direct marketing, at the time the information was originally collected. The Information Commissioner ²⁴ has issued guidance²⁵ on all of the above matters.

Under UK laws, businesses should check their emailing lists to avoid fines. Any existing mailing list that is a combination of business and personal email addresses may place directors at risk if a spam message is sent to an individual who has not consented or with whom there is no customer relationship. Offenders face a fine of £5,000 for every breach (juries may impose unlimited fines). However, the Information Commissioner and the DTI have indicated that discretion will be applied. Companies which can demonstrate that they adhered to the principles of the Data Protection Act 1998 when they first collected data are likely to avoid liability.²⁶

This regulation, however, only applies to the transmission of unsolicited communications by means of electronic mail to **individual subscribers**. "Individual" is defined to mean a living individual and includes an unincorporated body of such individual. **This means that it is legal for a company or spammer to send spam to corporate email addresses**. The All Party Parliamentary Internet Group ("APIG") believes that it is a very serious mistake in not prohibiting unsolicited business-to-business email. According to the Department of Trade and Industry ("DTI"), the decision was taken so that "legitimate business-to-business communication" was not hampered. The DTI insists that during its consultation on the new Directive, many businesses said that they did not want to lose email as a marketing tool. As far as Mauritius is concerned, it will have to be ascertained from the business community as to whether it is to be legal for a company to send spam to corporate email addresses?²⁷

²⁴ See www.informationcommissioner.gov.uk

²⁵ See <http://ico-cms.amaze.co.uk/DocumentUploads/IntroductiontoGuidance-Please Read This First.pdf>

²⁶ See www.informationcommissioner.gov.uk/eventual.aspx?id=786

²⁷ Email is considered by many as one of the "killer applications" for the growth of the Internet and therefore, electronic commerce. However, spam can pose a threat to the security and reliability of communications over the Internet.

E. Cookies and bugs

The problem with the use of cookies is that many users are unaware of cookies and of the fact that information is collected without knowledge or consent of the user, and may be used for direct marketing purposes.

Whether there are data protection implications in the use of cookies depends largely on what the cookie is designed to do. The least invasive type of cookies simply detects if someone has previously visited a site so that their preferences in relation to the site can be reset.²⁸ Other cookies will report back to a site all of a user's activities on the site including pages visited, products bought, etc. In many cases the use of cookies will amount to the collection of personal data on a user and will therefore have data protection implications.²⁹ The most significant implications will be ensuring that any personal data is processed (collected) fairly and lawfully and that the relevant data subject is provided with the specified information.³⁰ If the personal data gathered by cookies is subsequently used for the purposes of direct marketing then the data subject will have the right to object under section 11 of the Data Protection Act 1998 (DPA).³¹ More importantly, the PEC Regulations prohibit the use of personal data for direct marketing purposes unless prior consent of the data subject has been obtained.

The DPA lays down other specific conditions, which must be met to process personal data. These include that personal data must only be collected for specified, explicit and legitimate purposes; no further processing which is incompatible with the original, legitimate purpose is permitted; processing must be adequate, relevant and not excessive in relation to the purpose; and data must not be stored for longer than is necessary, etc. If personal data is collected and processed online, the Article 29 Working Party has recommended a set of minimum set of obligations for the data controllers to follow to ensure compliance with the Data Protection Directive.³²

The new EU Directive: Rules on Cookies

Recital 24 of the Directive on Privacy and Electronic Communications (DPEC)³³ recognises the use of cookies as part of the private sphere of users requiring protection under the European Convention on Human Rights. Thus, "[t]he use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned".

Besides, recital 25 provides:

²⁸ Rosemary Jay and Angus Hamilton, *Data Protection: Law & Practice* (2nd ed., 2003), p.656.

²⁹ *ibid.*

³⁰ *ibid.*

³¹ *ibid.*

³² See Recommendation 2/2001 on Certain Minimum Requirements for Collecting Personal Data Online in the European Union, adopted on May 17, 2001

³³ Directive 2002/58

"However, such devices, for instance so-called cookies, can be a legitimate and useful tool ... where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with directive 95/46/EC about the purposes of cookies or similar device ... Users should have the opportunity to refuse to have a cookie or similar device stored in their terminal equipment."

Also, Article 5(3) of the DPEC provides:

"Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller."

The combined effect of Recitals 24, 25 and Art. 5(3) is that:

- (a) cookies may only be used for legitimate purposes;
- (b) the subscriber or user concerned must be provided with clear and comprehensive information about the purposes of the processing. This information must be provided in accordance with the Data Protection Directive, which includes the requirement to state the data controller's identity; the purposes of processing; and any other information that, in the particular circumstances, is required to make the processing fair;
- (c) the subscriber or user concerned must be offered the right to refuse a cookie;
- (d) the information/opt-out opportunity may be offered on a one-off basis covering the initial connection and any further use of the cookie; the method for providing the information and dealing with the opt-out should be made as user-friendly as possible; and
- (e) services can be conditional upon acceptance of a cookie, if used for a legitimate purpose.

In addition, the Article 29 Working Party has recommended that the data controller will have to mention clearly the existence of automatic data collection procedures (cookies) before using such a method to collect any data.³⁴

The DPEC is implemented in the United Kingdom by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "**PEC Regulations**"), part of which came into effect on December 11, 2003. Regulation 6 provides:

- (1) Subject to paragraph (4), a person shall not use an electronic communications network to store information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.
- (2) The requirements are that the subscriber or user of that terminal equipment-
 - (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
 - (b) is given the opportunity to refuse the storage of or access to that information.
- (3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.
- (4) Paragraph (1) shall not apply to the technical storage of, or access to, information-
 - (a) for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or
 - (b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

The UK Information Commissioner has published guidance that provides his interpretation of the rules of the Regulations.³⁵ He reminded the service providers of the implication of cookies for data protection. The Information Commissioner states, "[w]here the use of a cookie type device does involve the processing of personal data, service providers will be required to ensure that they comply with the additional requirements of the DPA 1998. This includes the requirements of the third data protection principle which states that data controllers shall not process data that is excessive."³⁶

The Directive, however, seems to provide little guidance as to what information needs to be provided to the user, likewise the Regulations. Article 5(3) simply states "that the subscriber

³⁴ See Recommendation 2/2001 on Certain Minimum Requirements for Collecting Personal Data Online in the European Union, adopted on May 17, 2001.

³⁵ Information Commissioner, Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 2: Security, Confidentiality, Traffic and Location Data, Itemised Billing, CLI and Directories, pp.4-7.

³⁶ *ibid.* para.2.1

or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia*, about the purposes of the processing". The Data Protection Directive is specifically referred to in this provision and many other provisions of the Directive. So the information provided to users must be sufficient to enable a user to make an informed decision as to the use of cookies.

It is to be noted however that the Directive and the Regulations do not make a distinction between permanent and session cookies. Indeed whereas permanent cookies remain on the terminal equipment after closing the connection, session cookies, which may indeed in some cases be necessary for the functioning of the website, disappear at the end of the session. According to the Belgian data protection commission, whereas the use of session cookies may be considered in some cases as necessary and complying with the data protection principles, this is not always the case as regards the use of permanent cookies.³⁷

F. Spam-damages and enforcement

Regulation 30 creates a new civil right to damages with the claim lying against a person who contravenes any requirement in the Regulations. It provides that "a person who suffers damage by reason of any contravention of any of the requirements of these Regulations by any other person shall be entitled to bring proceedings for compensation from that other person for that damage". The Regulations also provide for a defence. Regulation 30(2) states that in proceedings against a person by virtue of this regulation, it shall be a defence to prove that he had taken such care as in all circumstances was reasonably required to comply with the relevant requirement.

Regulation 30(1) allows any party to bring an action for damages. It provides that "a person who suffers damage by reason of any contravention of any of the requirements of these Regulations by any other person shall be entitled to bring proceedings for compensation from that other person for that damage". The Regulations also provide for a defence. Regulation 30(2) states that in proceedings against a person by virtue of this regulation, it shall be a defence to prove that he had taken such care as in all circumstances was reasonably required to comply with the relevant requirement.

Clive Gringras pointed out that it would be unlikely for a single individual to be able to show that they had suffered substantial losses as the result of spam. However, groups of individuals, or ISPs on their behalf, might be in a better position to be able to show the true level of damage that had been incurred. He suggested that "super complaints" should be

³⁷ See Sophie Louveaux and Maria Veronica Perez Asinari, "New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector--Some Initial Remarks" [2003] C.T.L.R. 135

permitted, such as those that can be made by consumer organisations to the Office of Fair Trading under the Enterprise Act 2002.³⁸

By virtue of regulation 31, the enforcement powers are vested in the Information Commissioner. And the remedies for breach are contained in Pt V of the DPA and Schedules 6 and 9. Under s.40 of the DPA as amended by this regulation, the Information Commissioner is empowered to serve an enforcement notice on any person that the Commissioner is satisfied has contravened or is contravening any of the requirements of the Regulations. A person who fails to comply with the enforcement notice is guilty of an offence³⁹ and punishable by a fine, which is limited to £5,000 in the magistrates' court and unlimited in the crown court.

Where it is alleged that there has been a contravention, regulation 32 allows either the Office of Communications ("OFCOM") or a person aggrieved by the contravention of the requirements of the Regulations to make a request to the Commissioner for him to exercise his enforcement function. However, this does not mean that the enforcement function of the Commissioner can only be exercised upon request. It is exercisable whether or not there is a request.

As section 40 of the DPA requires, the Information Commissioner must be satisfied that a person has contravened or is contravening the requirements of the Regulations. It implies that there must be some kind of formal investigation before an enforcement notice is issued. The regulations in Schedule 1 require that the words "or distress" in section 40 be omitted. The implication is that in deciding whether to serve an enforcement notice, there is no need for the Information Commissioner to consider whether the contravention with the requirements of the Regulations has caused or is likely to cause distress to any person. Perhaps this is the recognition that spam causes distress and that no proof is needed.

In deciding whether to serve an enforcement notice, the Commissioner must consider whether the contravention has caused or is likely to cause any person damage.⁴⁰ This, however, does not mean that the Commissioner can only issue an enforcement notice in cases where damage has occurred. What it will probably mean in practice is that the Commissioner will feel more inclined to issue such a notice in the presence of damage and less inclined to do so in the absence of it. If this interpretation is incorrect, at minimum the provision makes it mandatory for the Commissioner to take into account whether the contravention has caused or is likely to cause any person damage.

³⁸ See APIG, Spam: Report of an Inquiry by the All Party Internet Group (October 2003).

³⁹ s.47 (1) of the DPA.

⁴⁰ s.40 (2) of the DPA.

Many argue that the Information Commissioner, enforcement notices and criminal penalties for failure to comply are not the answers to spam. Some consider an enforcement notice will be too little too late.⁴¹ APIG's finding deserves attention⁴²:

"We are very concerned by the evidence we heard with regard to enforcement and the Information Commissioner's own comments upon the DTI's new Regulations. We do not believe that he has been given the ability to act quickly and decisively to stop the sending of spam. We do not believe that waiting for an enforcement notice to be breached before financial penalties are applied is anything other than a recipe for spammers to 'try it on' until the authorities catch up with them."

THE UNITED STATES -

In an effort to address the problem of spam, the United States passed the "Controlling the Assault of Non-Solicited Pornography and Marketing Act," otherwise known as the CAN SPAM Act 2004.

The CAN SPAM Act provides criminal penalties for five main activities under certain circumstances for:

1. hijacking a computer and transmitting multiple commercial emails from that computer;
2. relaying or retransmitting multiple⁴³ commercial emails with the intent to deceive or mislead as to the origin of the messages;
3. falsifying header information in multiple commercial emails;
4. using false information to register for several email accounts or domain names and sending multiple commercial emails from such accounts or domain names; and
5. falsely representing oneself to be the registrant or successor in interest to several Internet Protocol ("IP") addresses and transmitting multiple commercial emails from those addresses.⁴⁴

The Act does not require that the commercial email be unsolicited for liability to attach.

In addition to the criminal provisions, the Act provides guidelines and enforcement mechanisms for other commercial email practices. These can be boiled down into a few key principles that mimic the criminal statute: entities sending a commercial email may not hide who they are, where their email is coming from, or what the message is about, and they must provide some way for recipients to request that they not be sent additional emails.

⁴¹ Mike Butler, "Spam--The Meat of the Problem" (2003) 19 Computer Law and Security Report 388

⁴² APIG, op.cit., para.53.

⁴³ The Act defines "multiple" as more than 100 emails in 24 hours, more than 1000 emails during a 30-day period, or more than 10,000 emails in a one-year period. Solicitors who send lesser volumes of email are not criminally liable

⁴⁴ In addition, the Act provides criminal sanctions for violation of its new rules regarding sexually explicit email.

The scope of email covered under the Act is extremely broad. "**Commercial email messages**" are defined as emails "**the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an internet website operated for a commercial purpose)**". The definition of "primary purpose" is, as yet, unclear, and may be interpreted as encompassing certain email communication not always thought of as commercial advertisements.

The requirements under the CAN SPAM Act are:

First, the Act prohibits transmission of commercial email, or a "transactional or relationship message", that contains or is accompanied by materially false or misleading header information. The Act defines "header information" as "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message."

"Transactional" and "relationship" emails are essentially emails the primary purpose of which is to continue a pre-existing commercial relationship. Transactional or relationship message emails are those having a primary purpose to:

- (a) facilitate, complete, or confirm a commercial transaction that the recipient previously agreed to enter;
- (b) provide warranty, product recall, safety, or security information used or purchased by the recipient;
- (c) notify the recipient of various changes or account balance information in relation to a subscription, membership, account, loan, or comparable ongoing commercial relationship;
- (d) provide information related to employment or a related benefit plan the recipient is involved in; or
- (e) to deliver goods or services to which the recipient is entitled according to previous transactions.

These types of emails must have a truthful header. "Materially" false or misleading header information is a low threshold under the Act, but if the "from" line accurately identifies the sender as the initiating source of the message, it will not be considered materially false or misleading.

Secondly, the Act bans sending email that contains a subject heading that the sender knew or should have known would be misleading as to the subject matter of the message. Thus, all subject lines should accurately reflect the contents of the message being transmitted.

Thirdly, commercial email must provide notice of the ability to opt-out of receiving future emails, and must clearly and conspicuously display a functioning return email address or other internet-based mechanism enabling the recipient to opt-out of future email messages from the sender. A "sender" for purposes of the Act is defined as the person who initiates such a message and whose product, service, or website is advertised or promoted in the message. Consequently, the opt-out provisions are directed towards the entity being promoted rather than a contractor acting on the behalf of that entity. Emails must also contain a valid physical postal address of the sender. The sender may specify in the message how the recipient must reply to opt out of future emails, and gives a permissive example under which an entity may provide the recipient with a list or menu from which the recipient may choose the types of email messages he or she wishes to continue to receive, so long as there is an option to opt out of all future commercial emails. The CAN SPAM Act provides a 10-day period to process a request to opt out, after which the transmitting entity may no longer send commercial emails falling under the opt-out request. An entity may resume sending commercial email to a recipient that subsequently consents to receive such email.

Fourthly, if the commercial email is unsolicited, it must contain an identification of the email as an advertisement or solicitation. This provision do not apply to emails being sent to customers who have actively requested to receive the email information from the sender or to emails that qualify as "transactional or relationship" emails. The Act provides no specific guidance as to how or where such information should be presented, except that both the identification of the email as an advertisement or solicitation and the opt-out notification must be clear and conspicuous.

Enforcement and Liability

Enforcement authority lies primarily with the Federal Trade Commission ("FTC"), which may enforce the Act as a violation of 15 U.S.C. 57a(a)(1)(B) as an unfair or deceptive act or practice. Internet service providers also have certain enforcement rights.

States may file civil actions on behalf of residents for violations of prohibitions concerning false or misleading header information or deceptive subject headings, failure to include a return address or internet-based mechanism to opt out of future commercial emails, transmitting commercial emails after a recipient has opted out, or failure to include the identification of the email as advertising, a notice that the recipient may opt out, or a valid postal address for the sender. If the state seeks damages, it may recover either the amount of

loss suffered by its residents or statutory damages. Statutory damages are up to \$250 per violation, with each individual email treated as a separate violation.

Aggravated damages, which can add up to treble the normal statutory damages, may be awarded if:

- (1) the violation is committed wilfully and knowingly; or
- (2) the activity included certain aggravating factors.

Aggravated offences include sending non-conforming commercial email where the recipient's email address was harvested by an automated means from a website or a proprietary online service operated by another individual and that included a notice that the operator will not give, sell, or otherwise transfer email addresses to other parties for the purpose of enabling others to send email to those addresses. Other aggravated offences include: (1) "Dictionary attacks" (obtaining email addresses by automated means of generating various alphanumeric combinations in hope of creating valid email addresses); (2) using scripts or other automated means for registering for multiple email or online user accounts to send, or enable another person to send, illegal commercial email; or (3) knowingly relaying or retransmitting illegal commercial email from a computer or network that has been accessed without authorisation.

Courts may reduce damages where the defendant implemented commercially reasonable practices and procedures designed to effectively prevent violations and the violation occurred despite such practices. Total statutory damages are limited to \$2,000,000 unless the violation is under §5(a)(1) regarding false or misleading header information. Actual damages for false or misleading header information are not capped. In the case of a successful action, the court may also award costs and attorney fees to the state.

When commercial email contains false or misleading header information, liability extends beyond the persons actually sending the email to those reaping the benefits of the email advertising. Thus, if a second entity promotes a first entity's commercial interests, liability attaches if the first entity:

- (1) knew or should have known that its commercial interests were promoted in such a message;
- (2) received or expected to receive an economic benefit from the promotion; and
- (3) took no reasonable action to prevent the email's transmission or to detect the transmission and report it to the FTC.

"Do-Not-Email" Registry

The CAN SPAM Act required the FTC to investigate the feasibility of a federal do-not-email registry, and to report to Congress on a plan and timetable for establishing the registry within six months of enactment. The FTC, however, subsequently determined that the establishment of a do-not-email registry would not be of benefit, and declined to establish the registry.

Mobile Service Subscribers

In contrast to the general opt-out approach to email, the Act requires the Federal Communications Commission ("FCC") to promulgate opt-in rules for mobile service subscribers. The rules must allow a mobile service subscriber to avoid commercial messages unless they have provided express prior authorisation.

Furthermore, the rules must allow a recipient of mobile service commercial messages to indicate electronically that they do not want to receive further commercial email from the sender. The FCC is also directed to consider whether providers of commercial mobile services are to be subjected to the prohibition and, if they are not made subject to the prohibition, to allow subscribers to opt out of future messages at the time of subscription or in any billing mechanism. Given the decreasing distinctions between mobile phones, personal data assistants, and various other internet connection devices, it is not entirely clear how this section of the Act will apply to new technologies.

AUSTRALIA

In April 2003 the Australian National Office for the Information Economy (NOIE) presented a review of the problem⁴⁵, which led to the Australian Spam Act 2003.

Spam is not defined in the Act. Indeed, the only places that the word spam occurs are in the title and the long title, which is "An Act about spam, and for related purposes". The website of the Australian Communications Authority which enforces the Act, defines spam as "*unsolicited commercial electronic messages regardless of their content*". The Act regulates unsolicited commercial electronic messages but this wide definition is subject to exceptions. If the definition was not subject to exceptions it would prohibit many wanted messages, such as those sent after the exchange of a business card or messages from educational institutions. The meaning of commercial electronic messages must be considered in light of the exceptions and the provisions relating to consent, which is discussed below. It is these

⁴⁵ NOIE--publications--"The spam final report—executive summary", www.noie.gov.au/publications/NOIE/spam/final_report/exec_sum.htm

provisions which allow the sending of legitimate commercial messages. The greater offensiveness of bulk spamming is covered by penalty provisions rather than in definition.

Commercial electronic messages are defined in section 6. They include all types of advertising and promotional messages unless regulations provide that a specified kind of electronic message is not a commercial electronic message for the purposes of the Act.

Under section 16(1) of the Spam Act 2003 a person must not send, or cause to be sent, a commercial electronic message that has an Australian link, and is not a designated commercial electronic message.

In a number of circumstances this has no application, namely:

- (a) if the relevant electronic account-holder consented to the sending of the message, or
- (b) if the person did not know; and could not, with reasonable diligence, have ascertained that the message had an **Australian link**, or
- (c) if the person sent the message, or caused the message to be sent, by mistake.

"Australian link" is defined in section 7. Generally this applies if a message either originated or was organised in Australia, or originates overseas but has been sent to an address accessed in Australia.

Section 16(6) is designed to cover spammers who send electronic messages to non-existent electronic or randomly generated addresses. It prohibits the sending of such messages if the person did not believe that the electronic address existed and the message has an Australian link.

Under section 17, a commercial electronic message must clearly and accurately identify the sender of the message. It must also include accurate information about how the recipient can readily contact the sender. Such information must be reasonably likely to be valid for at least 30 days after the message was sent.

Commercial electronic messages with an Australian link that are not designated commercial electronic messages must contain a functional unsubscribe facility. The specified electronic address must be capable of receiving the unsubscribe message, as well as a reasonable number of similar unsubscribe messages from other persons for at least 30 days after the message was sent (s.18).

Exceptions and consent provisions

There are a number of exceptions which are intended to accommodate messages of social worth. The exceptions are for:

- (i) "designated commercial electronic messages" as defined in Schedule 1. They must comply with section 17 and include information about the institution or organisation which authorised the sending of the message. Schedule 1, clauses 2 and 3 outline the range of messages and list a number of bodies that are authorised such as government, political parties, religious organisations, charities and educational institutions;
- (ii) messages that consist of no more than factual information and include accurate contact details of the sender (Schedule 1, clause 2);
- (iii) if the relevant electronic account-holder consented to the sending of the message (Schedule 2).

Schedule 2 provides that the expression "consent" means express consent; or consent that can reasonably be inferred from the conduct, and the business and other relationships, of the individual or organisation concerned.

The above exception list is lengthy and presumes that the range of messages is desirable, whereas that may not be the recipient's view. Clearly the last exception is desirable but consent will not ensure that the recipient will receive all wanted messages, such as invitations.

Address harvesting

Under Part 3:

- (i) "Address-harvesting software must not be supplied, acquired or used.
- (ii) An electronic address list produced using address-harvesting software must not be supplied, acquired or used."

Enforcement - Civil penalties

Civil penalties are covered in Part 4. The maximum penalties are substantial.

"A business that is found to be in breach of the Spam Act may be subject to a Court imposed penalty of up to \$220,000 for a single day's contraventions. If, after that finding, the business contravenes the same provision, they may be subject to a penalty of up to \$1.1 million."⁴⁶

⁴⁶ www2.dcita.govt.au/ie/publications/2004/02/spambusiness/spam_act

Injunctions may be granted under Part 5 in relation to contraventions of civil penalty provisions.

Under Part 6, a number of options are available to enforce the legislation. A person may give the Australian Communications Authority an enforceable undertaking in connection with a matter relating to:

- (a) commercial electronic messages; or
- (b) address-harvesting software.

In Australia, where the Federal Court is satisfied that the person has breached a term of the undertaking, the Court may make a range of orders, including an order directing the person to comply with that term of the undertaking, or to pay compensation or any other order that the Court considers appropriate.

KEY LEGISLATIVE ISSUES:

The key legislative issues are –

- (i) what types of messages should be regulated or prohibited, and who should be covered?;
- (ii) should an "opt-in" or "opt-out" approach be adopted?;
- (iii) should there be a requirement for electronic messages to include accurate details of senders, "unsubscribe" facilities, accurate header or subject lines, and labels if they are advertising or adult messages?;
- (iv) should there be rules against the supply, acquisition or use of "address-harvesting" lists and software?; and
- (v) what sanctions and/or remedies should be specified or be available?

APPENDIX 3: AN INTERNATIONAL COMPARISON OF SPAM CONTROL LEGISLATION

	Australia	United Kingdom	United States	South Korea	Japan
Relevant legislation	Spam Act 2003 Spam (Consequential Amendments) Act 2003	Electronic Commerce (EC Directive) Regulations 2002 (ECR 2002) Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR 2003)	CAN-SPAM Act of 2003	Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001	The Law on Regulation Transmission of Specified Electronic Mail (July 2002) Specific commercial transactions law (July 2002)
Definition of spam	The Act uses “commercial electronic messages”. S 5(1) defines “electronic messages” to include e- mails, instant messages and telephone calls. S 6(1) defines “commercial electronic message”.	ECR 2002 uses “unsolicited commercial communications sent by e-mail”: reg 8 ECR 2002. PECR 2003 uses “unsolicited communications for the purposes of direct marketing by means of electronic mail”: reg 22(2) PECR 2003. NB. Some obligations applicable to commercial communications generally.	The Act uses “commercial electronic mail messages”: s 5(a) (4) (A). Definitions of : – ‘electronic mail address’: s 3(5); and – ‘electronic mail message’: s 3(6).	Any commercial advertisement sent via e-mail, telephone, facsimile or other media prescribed by Presidential Decree transmitted to a consumer against consumer’s expressed rejection and therefore in violation of the law.	The law uses “unsolicited commercial e-mail”.
Extra-territorial jurisdiction	Certain provisions of the Act apply to commercial electronic messages with an Australian link, which is defined in s 7.	—	—	—	—
Opt-in vs. opt-out	<i>Opt-in</i> Section 16(1): Unsolicited commercial electronic messages must not be sent: – unless recipient has consented: s 16(2). – consent can be express or inferred: Para 2 of Sch 2.	<i>Opt-in</i> Person not to transmit unsolicited communications for the purposes of direct marketing by means of electronic mail unless recipient previously consented or sent at recipient’s instigation: reg 22(2) PECR 2003. Reg 22(3) PECR 2003: Exceptions: – existing customer or contact details obtained from recipient in previous negotiations; – direct marketing of similar products and services; and – unsubscribe facility at time contact details	<i>Opt-out</i> Prohibition of transmission of commercial electronic messages after objection: s 5(a) (4).	<i>Opt-out</i> Art 50 Restrictions on transmission of advertisement information: – any person shall be prohibited from transmitting advertisement information for the purpose of soliciting business against the addressee’s explicit rejection of such information.	<i>Opt-out</i> Transmission of specified emails to person who has requested not to receive them prohibited.

		collected and at each subsequent communication.			
Valid return e-mail address	Commercial electronic message to include accurate information about how the recipient can readily contact sender: s 17(1) (b).	E-mail communications for the purposes of direct marketing not to be transmitted where valid return address has not been provided: reg 23(b) PECR 2003.	Unlawful to send commercial electronic mail message that contains header information that is materially false or misleading: s 5(a) (1) — — inclusion of return e-mail address: s 5(a) (3). — inclusion of physical address: s 5(a) (5) (iii). Secondary liability for businesses knowingly thus promoted: s 6.	Art 11 Ordinance of the Ministry of Information and Communication of the Act: — must have clear posting of addressor's name, telephone number and contact person.	(see under Labelling requirements) Unsolicited commercial e-mail must include sender's email address.
Functional unsubscribe facility	Commercial electronic messages must contain a functional unsubscribe facility: s 18(1).	Simple means of refusing use of contact details for the sending of electronic mail for the purposes of direct marketing to be provided at time contact details initially collected and at time of each subsequent communication: reg 22(3) (c) PECR 2003. Valid return address to which opt-out request can be sent: reg 23(b) PECR 2003.	Functional internet-based opt-out mechanism: s 5(a) (3). Inclusion of clear and conspicuous notice of opportunity to opt out: s 5(a) (5) (ii).	Art 11 Ordinance of the Ministry of Information and Communication of the Act: — must have clear instructions on how to reject future e-mails; — commercial advertisement senders must install toll-free numbers so that recipients may express their intention not to receive any spam in the future. Art 50(2) Restrictions on transmission of advertisement information: — to indicate matters concerning easy methods to reject receipt of future advert. information.	(see under Labelling requirements) Unsolicited commercial e-mail must include opt-out e-mail address.
Identify sender	Commercial electronic message to clearly and accurately identify sender: s 17(1) (a).	E-mail for the purposes of direct marketing not to be transmitted where identity of person on whose behalf communication is sent has been disguised or concealed: reg 23(a) PECR 2003. Commercial communications to clearly identify person on whose behalf it is made: reg 7(b) ECR 2002	Line identifying person initiating message to accurately not to be materially false or misleading: s 5(a) (1) (B) Secondary liability for businesses knowingly thus promoted: s 6.	Art 50(2) Restrictions on transmission of advertisement information: to indicate the following: — types of transmission and major contents in there; — name/ contact means of addressor.	Unsolicited commercial e-mail must include sender's name and address.
Labelling requirements	—	Unsolicited commercial communications to be identifiable as such as soon as it is received: reg 8 ECR 2002. Commercial communications to be clearly identifiable as commercial communications: reg 7(a) ECR 2002. Promotional offers, competitions or games and conditions to be	Prohibition of deceptive subject headings: s 5(a) (2). Inclusion of identifier that message is an advertisement or solicitation: s 5(a) (5) (i). Requirement to place warning labels on spam containing sexually oriented material: s 5(d).	Art 11 Ordinance of the Ministry of Information and Communication of the Act: — initials 'ADV' must be included in mail header	Obligation of labelling for senders of specified email: 1. Identification as specified e-mail; 2. Sender's name/ address; 3. Sender's e-mail address; 4. Opt-out e-mail address.

		clearly identified: s 7(c) & (d) ECR 2002.			
English language requirement	—	—	—	Art 11 Ordinance of the Ministry of Information and Communication of the Act: – encourages Korean companies and individuals to insert English language buttons or links with which foreign users may reject and block future spam from the same source.	—
Dictionary attacks	Person must not send commercial electronic message to a non-existent electronic address that he has no reason to believe that exists: s 16(6).	—	Prohibition to transmit unlawful commercial electronic mail messages using, or to provide list of addresses obtained through, dictionary attacks: s 5(b) (1) (A) (ii).	Art 50(6) Restrictions on transmission of advertisement information: prohibition on use of software or other technical equipment that generate contacts by collating with numbers, codes or characters.	Prohibition of mail transmission utilizing the program that generates random fictitious e-mail addresses Telecommunications carriers are permitted not to provide a volume of e-mail transmission services if the emails include random fictitious addresses.
Address harvesting	Address-harvesting software and harvested-address lists must not be: – Supplied: s 20(1); – Acquired: s 21(1); or – Used: s 22(1).	—	Prohibition to transmit unlawful commercial electronic mail messages using, or to provide list of addresses obtained through, address harvesting: s 5(b) (1) (A) (i).	2 of Art 50: Prohibition of harvesting e-mail addresses from websites, etc.: – no person shall harvest e-mail addresses from websites that expressly prohibit automatic harvesting with software or other equipment; – no sale or circulation of e-mail addresses in violation of (1); – no person shall knowingly use e-mail addresses that have been automatically harvested for purpose of sale/ exchange regarding transmission of advertisement information. Art 50(2) Restrictions on transmission of advertisement information: to indicate source of e-mail address harvested.	—
Automated throwaway accounts	—	—	Unlawful to use automated means to register for multiple e-mail accounts from which to transmit unlawful commercial electronic mail messages: s 5(b) (2).	—	—
Right to commence	“Victim” i.e. person who has suffered loss or damage, may	Person who suffers damage entitled to bring proceedings for	State Attorney-General may bring civil action: s 7(f). ISP	—	—

legal action	apply to court for compensation: s 28. Australian Communications Authority (ACA) may apply to court: ss 26, 28, 29.	compensation: reg 30 PECR 2003.	adversely affected may bring civil action: s 7(g).		
Remedies	The main remedies for breaches of the Act are: – civil penalties: Pt 4 – compensation to victim: s 28 – injunctions: Pt 5.	Compensation for person who suffers damage: reg 30 PECR 2003. Enforcement under Part V of the Data Protection Act 1998: reg 31 PECR 2003. – enforcement notice: reg 32 (failure to comply: offence (s 47))	Enforcement by Federal Trade Commission: – fines & imprisonment: s 1037(b) Chapter 47 of title 18, United States Code; and – forfeiture: s 1037(c) Chapter 47 of title 18, United States Code. Civil action by States: – injunction: s 7(f) (2); and – statutory damages: s 7(f) (3). Civil action by ISP: – injunction: s 7(g) (1) (A) – damages of actual monetary loss: s 7(g) (a) (B) – statutory damages: s 7(g) (3).	Fines generally.	Administrative Orders by Minister to keep law Fines up to 500,000 yen assessed on failure to observe Administrative Order
Persons who may be liable	Sender of commercial electronic messages. Any person who: - aids, abets, counsels or procures a contravention; - induces, whether by threats or promises or otherwise, a contravention; - in any way, directly or indirectly, is knowingly concerned in or party to, a contravention; or - conspires with others to effect a contravention.	Any person transmitting or instigating the transmission of a communication: PECR 2003	Sender of commercial electronic mail message. Any person who initiates/ procures transmission of commercial electronic mail message (s. 5)	Any person transmitting advertisement information.	Sender.
Multi-pronged approach	Australian Communications Authority (ACA) has the following additional functions: – education: s 42(a); – research: s 42(b); and – international co-operative arrangements: s 42(c).	No formal regulatory framework mandated - but appropriate industry filtering initiatives encouraged.	Technical solution: - black lists - e-mail filters promoted. Self regulation.	Art 50(4) Restrictions of service for transmitting advertisement: – ISP may deny certain services at their discretion where there is or will be obstruction caused by repetitive transmission spam, or if users don't wish to receive such information; – ISP shall indicate its right of denial in its contract; – Where ISP intends to deny certain service, it shall give notice to user of that service or persons having an interest.	ISPs may take measures to suspend service usage for spammers. ISPs to provide email filtering services. Email marketing groups to make guidelines for email advertisements. Future plans to promote self-regulatory and technical solutions by ISPs and mobile operators. Awareness actions.

APPENDIX 4: KEY TIPS FOR USERS

Help Prevent Spam

1. Be careful who you give your email address to.

Only give your email address to individuals and organisations that you want to communicate with and that you trust to keep it private.

2. Consider using two or more email addresses.

Use separate personal and business emails and use one for systems that might result in spam. This can reduce sifting through emails to find the relevant ones. Many ISPs (Internet Service Providers) allow customers to have multiple email addresses as part of their standard package. Many other companies offer free email addresses.

3. Choose a less vulnerable email address.

An email address is a unique reference to a person and as such people want it to not only reflect their persona, but also be memorable.

Unfortunately, these justifiable desires help the spammer in attempting to guess email addresses. For example, if your name is John Smith, a spammer will try john.smith@..., j.smith@..., jsmith@..., smithj@..., smith.j@...,

The spammers' systems simply take every dictionary entry and try it in various combinations with every other dictionary entry. They will also introduce letters and numbers into the combinations because people might use birthdates, ages or even lucky numbers in their email addresses.

If you are willing to use an impersonal email address to attempt to reduce the problem of spam, use an address that does not have any potential dictionary entries in it.

4. Don't advertise your email address.

Don't advertise your address on search engines, contact directories, membership directories or web pages.

If you use chat systems, never expose your email address on the listing or directory and never disclose it to anyone other than friends.

5. Check Privacy Policies and Marketing Opt-Outs Carefully.

If you are purchasing a product on-line or subscribing to a service, check the company's privacy policy before giving your email address or any other private information.

Consider carefully how the company uses private information and the restriction they have regarding distribution and use of private information within their own company and with other external companies.

Help reduce spam: I already get spam, what can I do about it?

1. Consider that in some cases it may not be appropriate to reply to the spam.

Under some circumstances, the senders are allowed to send marketing emails until the recipient chooses to 'opt out'. You should, however, bear in mind that most spam email originate from outside Mauritius.

Replying to spam can indicate that your email address is live and can encourage some spammers to send you even more emails.

2. If your email system has a facility to tell when an email has been delivered or read, turn it off.

Delivery and read receipts can identify your email address as active and will result in even more spam.

3. Don't click on the adverts in spam emails.

By clicking on spammers' web pages, you are identifying your email as a live address and may make yourself a target for even more email. Graphics and images in spam emails can also reveal other private information such as your ISP address.

4. Use client side filters

Client filters are software programs that work in conjunction with your email package to sift through new emails to separate the spam from the wanted emails. Most packages can claim a high success rate. The downside is that they sometimes block good email as well as spam and emails still have to be downloaded before they can do their job. Spam filters are being further developed all the time, you can [search the Internet](#) for a spam filter that is suitable for you.

5. Use ISP based filters.

Many ISPs offer solutions that can be very effective at blocking spam. They use a combination of content examination and blacklists to restrict the amount of spam reaching the reader. Again, the downsides are that they sometimes block good email as well as spam and there is also usually a cost involved. For further information on the services that are available to you, please check with your ISP.

6. Keep your systems well maintained.

Just as cars are serviced and car manufacturers fix problems, your computer system should also be maintained. Most software companies issue product updates and patches that fix known problems with their software. Hackers and spammers can exploit these problems. Updates to manufacturers' software are generally available through their websites and are usually free to download and install.

Most users should also consider using anti-virus software to protect against virus programs that can destroy computer files.

APPENDIX 5: E-MAIL MARKETING BEST PRACTICE

Background

Following the recommendation from the Anti-Spam committee regarding the need for companies involved in electronic marketing activities to adopt certain best practices, the following document has been developed which presents a set of best practices for electronic marketing (For most purposes, this may be restricted to email, but other methods of delivering spam do exist, including the Short Messaging Service, or SMS, Voice over IP, mobile phone multimedia messaging services, instant messaging services). These best practices will help Mauritian organisations adopt spam-free marketing techniques and will make it clear that spam plays no legitimate role in email marketing originating from Mauritius or Mauritian companies.

Increasingly, Internet service providers (ISPs) and email service providers (ESPs) are looking for ways to stop spam by using filtering, black⁴⁷ and white⁴⁸ lists. As a result, they are inadvertently blocking legitimate email messages before they reach their intended recipients. Organisations are encouraged to adopt the best practices cited here as a way to ensure that their own legitimate email messages reaches their intended recipients.

These best practices are not legally binding, but are intended to complement existing Mauritius laws that govern spam, privacy, email marketing and marketing to children. For example, the *Data Protection Act 2004* (DPA) establishes the obligations of those who collect, use and discloses personal electronic-mail addresses. Organisations should make themselves aware of these laws and govern their activities accordingly.

The best practices, along with explanatory notes and illustrative examples, are outlined in the following sections.

⁴⁷ A list of IP addresses, domains or email addresses from which email is not accepted. The most common form of black list is a Domain Name System black list (DNSBL), a list of IP addresses distributed via the Internet's DNS. Popular DNSBLs include the Spamhaus Black List (SBL), the Composite Black List (CBL) and the original DNSBL, called the Mail Abuse Prevention System (MAPS) Reverse Black List (RBL). Contrast this with "white list."

⁴⁸ A list of email addresses or IP addresses from which a mail server is configured to accept incoming mail. White lists can be useful as one part of an email filtering system. Compare this with "black list."

Recommended Best Practices

1. Marketing email should only be sent to recipients who have provided their consent to receive such information.

This best practice directly relates to the sending of unsolicited commercial email for the purposes of soliciting goods and/or services. If organisations have not obtained the express consent of recipients prior to sending these types of email messages, then they are sending spam.

If the organisation has an existing business relationship with the intended recipient, it is sufficient to rely on implied consent. Under existing Mauritius law, where an individual has entered a contest, made a donation, or registered online for a product, newsletter, etc.; has provided their email address as part of the transaction; and has been provided with the opportunity to opt out⁴⁹ of receiving further marketing email messages, and has not done so, the organisation has the implied consent to email the individual. When using this form of consent, the marketer should explain to the intended recipient why they are receiving the email. In the follow-up communications, the organisation must provide the individual with an opportunity to opt out of receiving further marketing emails (see Best Practice #2).

Organisations should not send email marketing messages to recipients who have indicated they do not wish to receive email messages from the organisation. While an organisation may send email messages during an existing business relationship, they must honour an individual's request to be removed from email marketing lists at any time. This can be accomplished by providing an opt-out opportunity in every message sent (see Best Practice #2).

There is an exception for sending email messages outside of an existing business relationship, or to a customer whose file has become inactive. If the organisation has service, warranty or product-upgrade information, or if there are health and safety issues related to a product purchase, the organisation may send email messages to its customers. Organisations should use discretion in doing so, however, as customers may view this email as spam if the organisation uses it as an opportunity to up-sell or cross-sell products.

⁴⁹ Also called "negative consent." The organization presents the individual with an opportunity to express non-agreement to an identified purpose. Unless the individual takes action to "opt out" of the purpose — that is, say "no" to it — the organization assumes consent and proceeds with the purpose. The individual should be clearly informed that the failure to "opt out" means that the individual is consenting to the proposed use or disclosure of information.

- 2. In all marketing email, recipients must be provided with an obvious, clear and efficient email or web-based means to opt out of receiving any further business and/or marketing email messages from the organisation.**

In all email messages to current customers, organisations must include an opportunity for the recipient to opt out. This opportunity should not be buried in the email message and must be website- and/or email-enabled. The language used should be as simple as: “If you no longer wish to receive marketing offers from this organisation, please [click here](#) or email **info@ABCcompany.com**.”

The process for opting out should be simple and straightforward, and organisations should confirm by email that the opt-out request has been or will be followed through without requiring further action by the consumer.

Because of the sensitivities associated with email communications, and the problems caused by spam, organisations should honour an email opt-out request as final and remove that individual from their marketing lists until such time as the individual opts to receive email messages again.

- 3. The internal process used to obtain consent should be clear and transparent. Organisations should keep records of the type of consent obtained from recipients so that email lists can be scrubbed prior to campaign broadcasts.**

Organisations should ensure that they have the means to honour opt-out requests on a timely basis and to scrub their lists accordingly.

In addition, an internal process should be in place that records proof of consent, including the date, time, originating Internet protocol (IP) address and location (including URL), where the address collection occurred and whether consent was obtained via another medium (e.g. business card, contest form, telephone, verbal communication or credit card [e.g. through a paying subscription to a list]). Organisations should be able to provide this information to a recipient upon request.

- 4. Every email marketing communication should clearly identify the sender of the email. The subject line and body text in the communication should accurately reflect the content, origin and purpose of the communication.**

The identification of the sender and source of the email should be clearly and obviously specified and, whenever possible, placed above the fold (that part of the email that is visible without scrolling).

Example #1: Direct from organisation to subscriber

Date: Tue, 7 Feb 2006 07:32:02 -0400

From: "John Doe" <doe777@intnet.mu>

TO: "Joe Consumer" <joe999@intnet.mu>

Subject: Your e-bill is ready / Votre facture électronique est prête

Example #2: Third-party email service provider to subscriber on behalf of an organisation

From: "Pete Moss Publications" <bounces@petemoss.com> <v2user-13990-IXoyuP..CahrNet_0bkktg@mailier.carrier.com>

Subject: Business News 02/21/06

To: <joe999@intnet.mu>

Date: Sat, 24 Feb 2006 18:50:17 -0700

Even in cases where the content is accurately related to the subject line, organisations are cautioned against using subject lines that refer to "free offers" or "winning prizes." This is, in part, due to the fact that some spam filters use keywords such as these to signal that the message is spam.

- 5. Every email should provide a link to the sender's privacy policy. The privacy policy should explain the intended use and disclosure of any personal information that might be gathered through "clickstream"⁵⁰ means or other website monitoring techniques.**

Organisations are obliged under DPA to adopt a significant degree of transparency in disclosing their personal-information gathering and handling practices. A privacy policy might include the type of information collected and/or used; whether information is disclosed to third parties; the use of "cookies"⁵¹ or other passive means of data collection;

⁵⁰ The series of mouse clicks and related actions that a user makes while visiting a website. For an e-commerce website, a clickstream might include browsing the catalog, putting items into a virtual shopping cart, providing payment and shipping information, and then entering the order.

⁵¹ A small data file created by a web server and stored on a user's computer. Cookies are a way for websites to identify users, keep track of users' preferences and recognize users who are revisiting the website. By keeping user histories, cookies let websites tailor pages and create custom experiences for individuals. Depending on how the web server is programmed, cookies may also contain personal information, such as site passwords and account numbers.

and security, accountability and enforcement procedures (see Annex #1 for sample privacy policy).

Organisations must make the information on their online information-gathering processes readily available in one comprehensive privacy policy on their websites. The privacy policy should also include an active link to an opt-out mechanism.

6. Marketers, list brokers and list owners should take reasonable steps to ensure that the addresses on their email lists were obtained with the proper consent.

Organisations, list brokers and list owners should share responsibility for sending email to recipients who have not given appropriate consent to receive these messages. Where an organisation, list broker or list owner knew or should have known that the proper consent was not obtained, they could be accountable. Reasonable steps that an organisation can take to ensure clean lists include:

1. Reviewing the privacy policy of the broker/owner of the list;
2. Put in place opt-in procedures to validate the email addresses in his possession so that the recipient can choose to opt-out;
3. Having the broker or owner sign a contract warranting that they have complied with the requirements of DPA.

7. Marketers should use a high degree of discretion and sensitivity in sending email marketing to persons under the age of majority, in order to address the age, knowledge, sophistication and maturity of this audience.

The ways in which those under the age of majority perceive and react to email marketing communications are influenced by their age and experience, and the context in which the message is framed. For example, email marketing communications that are acceptable for teenagers will not necessarily be acceptable for younger children. There is no way to guarantee the age of any person who signs up to an email subscriber list. Organisations should, therefore, use discretion and sensitivity when marketing to those under the age of majority, and should seek to engage parental permission in such communications.

First-party cookies are ones created by the website you are visiting. Third-party cookies are created by a website other than the one you are currently visiting, most often a third-party advertiser on that site. Third-party cookies let advertisers determine whether an individual user is visiting multiple websites that display the advertiser's ads, and are often considered a privacy risk. Modern web browsers offer options to refuse all cookies, to refuse third-party cookies and/or to accept or refuse cookies from specified websites.

- 8. When the content of an email is adult in nature the sender must — prior to sending the communication — verify that the recipient is of age to legally receive and view such content.**

Adult content includes material related to gaming and gambling, tobacco, alcohol, firearms and other weapons.

- 9. Organisations should have in place a complaint-handling system that is fair, effective, confidential and easy to use.**

Any complaints from individuals regarding the use of their email address should be dealt with courteously and within a reasonable time frame. Under the DPA⁵² Section 30 Subsection (2), the data controller shall stop the processing of personal data of the data subject, for the purposes of direct marketing, as soon as reasonably practicable and in any event not more than 28 days after the request has been received.

- 10. Organisations may disclose the email addresses of existing customers to third-party⁵³ affiliates or within a family of companies if:**

- They have consent to do so;
- They are using the addresses for purposes consistent with their collection as mentioned in their privacy policy (i.e. for marketing related to the original purchase or to provide services related to that purchase);
- It is transparent to the recipient why they are receiving email communications;
- There is an easy-to-use way to opt out of receiving further email communications.

Organisations may only disclose customers' email addresses to an affiliated third party or within a family of companies for cross-marketing purposes if they offer these customers an easy-to-use opt-out opportunity before disclosing the email address.

It must be transparent to customers why they are receiving additional, related marketing offers (e.g. under a company brand). The organisation should not assume that customers understand a corporate relationship or structure.

⁵² THE DATA PROTECTION ACT 2004

⁵³ "Third party" refers to an organisation corporately distinct from that with which the customer originally did business (list rental company), including an organisation corporately related to the original organisations (or charity) or part of the same group, where the relationship would not be apparent to the customer. Third parties do not include data processors operating on behalf of the organisation with whom the individual has established a business relationship

APPENDIX 6: LONDON ACTION PLAN

THE LONDON ACTION PLAN

On International Spam Enforcement Cooperation

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.

Global cooperation and public-private partnerships are essential to spam enforcement, as recognized in various international fora. Building on recent efforts in organizations like the Organisation for Economic Cooperation and Development (OECD) and the OECD Spam Task Force, the International Telecommunications Union (ITU), the European Union (EU), the International Consumer Protection Enforcement Network (ICPEN), and the Asia-Pacific Economic Cooperation (APEC), the Participants issue this Action Plan. 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. The Participants also open the Action Plan for participation by other interested government and public agencies, and by appropriate private sector representatives, as a way to expand the network of entities engaged in spam enforcement cooperation.

A. 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:

1. Designate a point of contact within their agency for further enforcement communications under this Action Plan.
2. 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.
3. Take part in periodic conference calls, at least quarterly, with other appropriate participants to:
 - a. Discuss cases.
 - b. Discuss legislative and law enforcement developments.
 - c. Exchange effective investigative techniques and enforcement strategies.

- d. Discuss obstacles to effective enforcement and ways to overcome these obstacles.
 - e. 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.
 - f. Participate as appropriate in joint training sessions with private sector representatives to identify new ways of cooperating and to discuss spam investigation techniques.
4. Encourage dialogue between Agencies and appropriate private sector representatives to promote ways in which the private sector can support Agencies in bringing spam cases and pursue their own initiatives to fight spam.
 5. Prioritize cases based on harm to victims when requesting international assistance.
 6. Complete the OECD Questionnaire on Cross border Enforcement of Anti-Spam Laws, copies of which may be obtained from the OECD Secretariat.
 7. 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.

B. 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:

1. Designate a single spam enforcement contact within each organization, who would coordinate with spam enforcement agencies on requests for enforcement-related assistance.
2. 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.
3. 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:

- a. 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.
- b. 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.

4. 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:

- a. What kind of information do you provide about potential spammers to domestic law enforcement agencies and under what circumstances?
- b. What kind of information would you provide about potential spammers to foreign law enforcement agencies and under what circumstances?
- c. How do you recommend that spam enforcement agencies submit requests for assistance to you?

C. 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:

1. 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.
2. Set up the conference calls mentioned in paragraph A.3.
3. Provide a contact for further communications under this Action Plan.

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

D. 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.

This Action Plan is meant to be a simple, flexible document facilitating concrete steps to start working on international spam enforcement cooperation. It is expected that the collective work program under this Action Plan may be refined, and if necessary changed by the participants, as new issues arise.

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.

APPENDIX 7: ANTI-SPAM ACTION PLAN

1. General Awareness For Users, Public Sector and Businesses

S/N	Action Item	Owner	Partner	Frequency	Outcome	Time Frame
1.1	Anti-Spam Day	NCB	Ministry of IT and Telecommunications, ICT Authority	Annual	Kick start activities for Anti-Spam Initiatives and awareness.	1 st June 2006
1.2	Common Anti-Spam Slogan	NCB	ACT, MITIA and ICT Authority		Key tips to help users protect themselves and fight spam will be disseminated to different stakeholders to be published on their websites and in the media	1 st June 2006
1.3	Anti-Spam Awareness Sessions for workers	Mauritius Employer Federation (Private sector) NCB and Ministry of IT and Telecommunications – IT Security Unit (Public Sector)		Ongoing	Provide anti-spam awareness sessions for the employees.	As from June 2006
1.4	Anti-Spam Programme on TV	NCB	ACT, Mauritius IT Industry Association, ICT Authority, ISPs, and MBC		Illustrate the problem of spamming and measures that users should adopt	10-15 minute video footage to be aired on TV – around July 2006
1.5	Anti-Spam Awareness Sessions students and general public	NCB	Ministry of IT and Telecommunications, ICT Authority, Internet Child Safety Foundation, Internet Society	Ongoing programme through NCB IT Coach facility	Disseminate information and best practices for end users with regards to fighting spam.	Monthly – From June 2006.
1.6	Setting up of Anti-Spam Website	NCB	Ministry of IT and Telecommunications, ISPs, ACT and MITIA		Provide information about anti-spamming measures and guidelines, anti-spam	June 2006

S/N	Action Item	Owner	Partner	Frequency	Outcome	Time Frame
					legislation, facilities to report spam and latest developments in spamming for different audiences, such as general public, students, SMEs and IT professionals.	
1.7	Publication and Dissemination of anti-spam information to consumers	ISP			Include information about anti-spam measures for their customers when issuing their invoices	Starting June 2006
1.8	Publication and Dissemination of anti-spam brochures and guidelines	NCB	Ministry of IT and Telecommunications, ICT Authority, ACT, Mauritius Chamber of Commerce and Industry, Mauritius IT Industry Association, Consumer Associations		Educate people about the problem and what measures they can implement in order not fall victim to spam.	One Brochure for General Public and One Anti-Spam Guide for Consumers each year – June 2006
1.9	Information about spamming to be included in the school curriculum at the Secondary level	Ministry of Education and Human Resources	Ministry of IT and Telecommunications, NCB, ACT, ICT Authority, MIE		Include in the school curriculum at the secondary level, information about what is spamming and what measures students need to be aware of in relation to it	Updated IT curriculum – November 2006
1.10	Organisation of technical workshops – Dissemination of Best Practices for IT Professionals	NCB	ACT and MITIA	Yearly	Disseminate best practice information on protecting e-mail servers against spam and other anti-spam related technology solutions	2 workshops for IT Professionals – June 2006 and March 2007
1.11	Spam Study	NCB	ICT Authority, ACT and MITIA	Annual	Assess awareness of users about the spam	2 studies – 1 towards general

S/N	Action Item	Owner	Partner	Frequency	Outcome	Time Frame
					problem and the effectiveness of the measures that have been implemented	users & 1 towards businesses

2. Guidelines for ISPs and Other Commercial Organisations

S/N	Action Item	Owner	Partner	Frequency	Outcome	Timeframe
2.1	Adoption of Industry Best Practice Guidelines by ISPs and Network Operators	ICT Authority	ISPs and network operators		Adopt the best practices mentioned in Appendix 1, which will help reduce spam and related threats.	June 2006
2.2	Best Practices for E-Mail Marketing	Mauritius Chamber of Commerce and Industry	NCB, ICT Authority, Consumer Associations, Advertising Association, Ministry of Industry, Small and Medium Enterprises and Commerce, Ministry of IT and Telecommunications		Commercial organizations engaged in e-mail marketing to implement the proposed guidelines at Appendix 5	July 2006
2.3	ISPs and service providers to implement measures to prohibit spamming activities on their networks	ACT	NCB, ISPs and service providers, ICT Authority, Ministry of IT and Telecommunications		Adopt and enforce Acceptable Use Policies (AUPs) that clearly prohibit spamming activities on their networks	August 2006
2.4	Guidelines to limit the problem of open relays	NCB	ISPs and service providers, ICT Authority		Implement recommendations of the Committee.	August 2006

3. Legal Framework

S/N	Action Item	Owner	Partner	Frequency	Outcome	Timeframe
3.1	Review of legal framework and drafting of	Ministry of IT and Telecommunications	NCB, ICT Authority, ISPs, ACT, MITIA, MCCI, JEC		Anti-Spam Legislation	February 2007

	legislation for Anti-Spam				
--	---------------------------	--	--	--	--

4. International Co-operation

S/N	Action Item	Owner	Partner	Frequency	Outcome	Timeframe
4.1	Engage in Multilateral initiatives – London Action Plan	Ministry of IT and Telecommunications	NCB, ICTA, ISPs, ACT, MITIA, MCCI, JEC		Signature of London Action Plan	September 2006
4.2	Engage in Bilateral initiatives <ul style="list-style-type: none"> - Australia - United States 	Ministry of IT and Telecommunications	NCB, ICTA, ISPs, ACT, MITIA		Signature of agreement with Australian and American Governments	March 2007
4.3	Participation in International Forum at the Level of ITU and African ISP Association	NCB	ACT, ICT Authority, ISPs, MITIA and Ministry of IT and Telecommunications	Ongoing - Quarterly	Working group on International Co-operation in the Monitoring Framework proposed to submit position papers for consideration at the level of the ITU and African ISP Association	As from July 2006

5. Monitoring of Action Plan

S/N	Action Item	Owner	Partner	Frequency	Outcome	Timeframe
5.1	Setting Up of Central Co-ordinating Body and Working Groups	NCB	Ministry of IT and Telecommunications, ICT Authority, ISPs, ACT, MITIA, MCCI, JEC	Monthly meetings	Monitor implementation of actions and review of action plan	May 2006

ACRONYMS

ACA	-	Australian Communications Authority
ACT	-	Association of operators in the ICT Industry namely Business Process Outsourcing (BPO)/Call Centre, Internet Service Providers (ISP) and International Long Distance (ILD) providers
AFNOG	-	African Network Operating Group
ANOIE	-	Australian National Office for the Information Economy
APEC	-	Asia-Pacific Economic Cooperation
APIG	-	All Party Parliamentary Internet Group
APIG	-	All Party Parliamentary Internet Group
AUP	-	Acceptable Use Policies
CAN SPAM	-	Controlling the Assault of NON-Solicited Pornography and Marketing (US Act)
CAP	-	Committee of Advertising Practice
CBL	-	Composite Black List
CMC Act	-	Computer Misuse and Cybercrime Act 2003
DNS	-	Domain Name System
DNSBL	-	Domain Name System black list
DPA	-	Data Protection Act 2003
DPD	-	Data Protection Directive
DPEC	-	Directive on Privacy and Electronic Communications
DTI	-	Department of Trade and Industry
EC	-	Electronic Commerce
ESP	-	Email Service Provider
ET Act	-	Electronic Transactions Act 2003
EU	-	European Union
FCC	-	Federal Communications Commission
FTC	-	Federal Trade Commission
ICPEN	-	International Consumer Protection Enforcement Network
ICT Act	-	Information and Communication Technology Act 2001
IP	-	Internet Protocol
ISP	-	Internet Service Provider
ITU	-	International Telecommunications Unit
JEC	-	Joint Economic Council
LAN	-	Local Area Network
LAP	-	London Action Plan
MAPS	-	Mail Abuse Prevention System
MBC	-	Mauritius Broadcasting Cooperation
MCCI	-	Mauritius Chamber of Commerce & Industry
MIE	-	Mauritius Institute of Education
MITIA	-	Mauritius IT Industry Association
MMS	-	Multimedia Message Service
NCB	-	National Computer Board
NDN	-	Non-Delivery Notices
OECD	-	Organisation for Economic Co-operation and Development
OFCOM	-	Office of Communications
OPP	-	Online Privacy Policy
PEC	-	Privacy and Electronic Communications
PECR	-	Privacy and Electronic Communications Regulations
RBL	-	Reverse Black List
RFC	-	Request For Comments
SBL	-	Spamhaus Black List
SME	-	Small And Medium Enterprise
SMS	-	Short Message System
SMTP	-	Simple Mail Transfer Protocol
SPF	-	Sender Policy Framework
SWIP	-	Shared WHOIS Project
TWC	-	thiswebsite.com

UBE	-	Unsolicited Bulk E-mail
UCA	-	Unsolicited Commercial Advertising
UCE	-	Unsolicited Commercial E-mail
URL	-	Uniform Resource Locator
WSIS	-	World Summit for Information Society