# Unsolicited commercial e-mail (spam): integrated policy and practice

A thesis submitted to Middlesex University
in partial fulfilment of the requirement
for the degree of Doctor of Philosophy

**Evangelos Moustakas**

School of Computing Science
Middlesex University

January 2007

*ABSTRACT* 6
*ACKNOWLEDGEMENTS* 8

**CHAPTER 1 INTRODUCTION TO THE RESEARCH AREA 11**
**1. Introduction 11**
**2. The problem 11**
**3. Objectives of the research and contribution to knowledge 13**
**4. Spam stakeholder analysis 14**
**5. Research on anti-spam legislation 14**
**6. Technical anti-spam solutions 15**
**7. Corporate e-mail policies 16**

**CHAPTER 2 LITERATURE REVIEW 17**
**1. Introduction 17**
**2. Why spam is a problem 17**
**3. Initiatives to address the problem of spam 20**
3.1 Spammers – defenders of spam 20
3.2 Internet service providers (ISPs) 21
3.3 Government – legislation 22
3.3.1 Introduction 22
3.3.2 EU legislation 23
3.3.3 The position in the USA 25
3.3.4 The Canadian code for consumer protection in e-commerce 26
3.3.5 Spam-blocking law proposed in Japan 28
3.4 Technical approaches to blocking 29
3.4.1 Real-time blocking lists 29
3.4.2 Content filtering technologies 29
3.4.3 False positives 31
3.5 Marketing and ISP associations 32

**CHAPTER 3 METHODOLOGY 34**
**1. Introduction 34**
**2. Defining the problem of spam 36**
**3. The questionnaire (open survey) 37**
**4. Stakeholder analysis as a platform for an integrated approach 41**
**5. Anti-spam legislation 43**
**6. Technical aspects 45**
**7. Organisations – corporate e-mail policy 47**
**8. Academic visit in the USA – University of Illinois at Chicago 49**
**9. Summary 50**

CHAPTER 4 UNSOLICITED COMMERCIAL COMMUNICATION: SPAM 51

1. Introduction 51
2. What is unsolicited commercial communication? 51
3. The negative impact of UCE 53
4. A typology of spam 56
5. Spammers' techniques to select e-mail addresses and ways to tackle the problem 58
   - 5.1 The "munging" technique 58
   - 5.2 Make e-mail addresses indistinct in the .html source code 59
   - 5.3 Online contact forms 59
6. Spam and cyber fraud 59
7. Growth and negative impact of online fraud 60
8. Explaining phishing 61
9. Methods used by phishers 62
   - 9.1 Collecting information using html forms 62
   - 9.2 Trojan horses and malicious JavaScript 63
   - 9.3 Imitation of reputable companies' web-sites 63
   - 9.4 Fake reply e-mail address 64
   - 9.5 Fake secure connection 65
   - 9.6 How to catch the phish fast 65
   - 9.7 Link to web-sites that gather information 66
   - 9.8 The loopholes of the DNS 67
   - 9.9 Social engineering 67
10. Mechanisms for tackling phishing 68
    - 10.1 Identifying the participants in phishing 68
    - 10.2 Consumers' awareness and education 70
    - 10.3 The three-layer protection scheme 71
11. Summary and conclusions 71

CHAPTER 5 TOWARD AN INTEGRATED APPROACH 72

1. Stakeholder analysis 72
2. Mechanisms for tackling UCE 76

CHAPTER 6 ANTI-SPAM LEGISLATION 81

1. Introduction 81
2. The need for anti-spam legislation 81
3. Types of liability 82
4. A review of anti-spam legislation 83
   - 4.1 EU and UK legislation 84
     - 4.1.1 Key elements of the EU Directive 84
     - 4.1.2 Effectiveness of the EU Directive 86

4.2 US legislation – Can-Spam Act 2003 88
4.2.1 Key elements of the US legislation 88
4.2.2 Can the Can-Spam Act reduce spam? 90
4.3 Australia – Spam Act 2003 91
4.3.1 Key elements of the Australian legislation 91
4.3.2 Effectiveness of the Australian legislation 92
4.3.3 Spam and internet security information/education programme 94
4.4 Anti-spam legislation in Canada 94
4.4.1 Key elements of the Canadian legislation 94
4.4.2 Effectiveness of the Canadian legislation 97
4.5 Anti-spam law in Japan 98
4.5.1 Key elements of the Japanese legislation 98
4.5.2 Effectiveness of the anti-spam law in Japan 99
4.6 The situation in New Zealand 99

**5. Legal recommendations to combat spam 100**
5.1 Effective use of advances in IT 100
5.2 Penalties and enforcement 101
5.3 International cooperation among the legislative bodies 101
5.4 Global harmonisation in anti-spam legislation 102

**6 Summary and conclusions 102**

**CHAPTER 7 TECHNICAL ASPECTS 104**

**1. Introduction 104**

**2. Evaluation of anti-spam solutions 104**
2.1 First-generation anti-spam solutions 105
2.2 Second-generation anti-spam solutions 106
2.2.1 E-mail server-based anti-spam solutions 107
2.2.2 Client-side anti-spam solutions 107
2.2.3 Gateway-based anti-spam solutions 108
2.2.4 Outsourced anti-spam solutions 108
2.3 Bayesian filtering 109

**3. Summary and conclusions 110**

**CHAPTER 8 CORPORATE E-MAIL POLICIES 112**

**1. Introduction 112**

**2. E-mail threats 112**
2.1 Breach of confidentiality 114
2.2 Defamation and obscenity 114
2.3 Wasted time and resources 116
2.4 Contractual liability – liability for defective products 116
2.5 Intellectual property issues 117

**3. Spam and corporate e-mail policy 118**

**4. The structure of an e-mail policy 120**

**5. Inside the corporate e-mail policy 122**

5.1 General guidelines 122
5.2 Clarity of e-mail policy, corporate education and awareness 123
5.3 Establishment of netiquette policies for e-mail senders and receivers, both managers and staff 123
5.4 Personal use 124
5.5 Evidence and data retrieval 124
5.6 Disclaimer statement for outgoing e-mails 124
5.7 E-mail confidentiality 125
5.8 Level of monitoring 125
5.9 Informing employees and recipients about e-mail monitoring 126
5.10 Cross-reference to relevant corporate policies 127
5.11 Breach of e-mail policy 127

**6. Implementation issues and policy changes and updates 127**
6.1 Implementation 127
6.2 Updating an e-mail policy 128

**7. The corporate e-mail policy for Atlantic Supermarkets SA, Greece 129**

**8. Summary and conclusions 133**

**CHAPTER 9 SUMMARY, CONCLUSIONS AND FURTHER WORK 134**

**1. Summary 134**
1.1 Unsolicited commercial e-mail – spam 135
1.2 Anti-spam legislation 135
1.3 Technical anti-spam solutions 136
1.4 Organisations and corporate e-mail policy 136

**2. Conclusions and contribution to knowledge 137**

**3. Further work 139**

**REFERENCES 140**

**APPENDIX A QUESTIONNAIRES 154**

**1. How users react to spam 154**

**2. Atlantic Supermarkets 156**

**APPENDIX B INTERVIEWS 157**

**APPENDIX C PUBLICATIONS 160**

**APPENDIX D SPAM WORKSHOPS AND CONFERENCES 164**

**APPENDIX E PRESENTATIONS 165**

**APPENDIX F LIST OF ANNOTATIONS 166**

## List of tables


| | | |
|---|---|---|
| Table 1 | Stakeholder analysis for UCE | 42 |
| Table 2 | Signal detection theory (statistical decision) | 46 |
| Table 3 | Types of spam: Federal Trade Commission | 52 |
| Table 4 | Types of UCE: Federal Trade Commission | 52 |
| Table 5 | Problems associated with spam | 55 |
| Table 6 | Proposed typology of UCE | 56 |
| Table 7 | The major differences between spam and phishing | 62 |
| Table 8 | Stakeholder analysis for phishing | 69 |
| Table 9 | Mechanisms for containing UCE: stakeholders and potential responses | 77 |
| Table 10 | How to tackle spam: the integrated scenario | 80 |
| Table 11 | Anti-spam legal environment | 84 |
| Table 12 | The major elements of the Canadian anti-spam statutes | 97 |
| Table 13 | Corporate e-mail threats and e-policy initiatives | 118 |
| Table 14 | Identifying e-mail threats in the corporate e-mail policy | 120 |


## List of figures


| | | |
|---|---|---|
| Figure 1 | The level of spam in the EU (2002) | 18 |
| Figure 2 | How do you consider spam? | 54 |
| Figure 3 | Who do you think is the most appropriate to handle spam? | 54 |
| Figure 4 | How many e-mails do you get on average per day using web-mail account? | 55 |
| Figure 5 | Phishing case I: html forms | 63 |
| Figure 6 | Phishing case II: paypal logo | 64 |
| Figure 7 | Phishing case III: TRUSTe symbol | 64 |
| Figure 8 | Phishing case IV: fraudulent reply addresses | 64 |
| Figure 9 | Phishing case V: fraudulent web-sites use https:// | 65 |
| Figure 10 | Phishing case VI: ebay | 65 |
| Figure 11 | Phishing case VII: Citibank | 66 |
| Figure 12 | Phishing case VIII: MSN | 67 |
| Figure 13 | Key stakeholders in the UCE process | 76 |
| Figure 14 | Brightmail: the Probe Network concept | 106 |
| Figure 15 | Infrastructure of path used by in/out-bound spam | 107 |
| Figure 16 | IDC's spam study, 2003 | 113 |
| Figure 17 | How many e-mails do you get on average per day through your business e-mail account? | 129 |
| Figure 18 | What are your actions in response to spam? | 129 |

# ABSTRACT

The internet offers a cost-effective medium to build better relationships with customers than has been possible with traditional marketing media. Internet technologies, such as electronic mail, web sites and digital media, offer companies the ability to expand their customer reach, to target specific communities, and to communicate and interact with customers in a highly customised manner. In the last few years, electronic mail has emerged as an important marketing tool to build and maintain closer relationships both with customers and with prospects. E-mail marketing has become a popular choice for companies as it greatly reduces the costs associated with previously conventional methods such as direct mailing, cataloguing (i.e. sending product catalogues to potential customers) and telecommunication marketing. As small consumers obtain e-mail addresses, the efficiency of using e-mail as a marketing tool will grow. While e-mail may be a boon for advertisers, it is a problem for consumers, corporations and internet service providers since it is used for sending 'spam' (junk-mail). *Unsolicited commercial e-mail (UCE)*, which is commonly called *spam*, impinges on the privacy of individual internet users. It can also cost users in terms of the time spent reading and deleting the messages, as well as in a direct financial sense where users pay time-based connection fees. Spam, which most frequently takes the form of mass mailing advertisements, is a violation of internet etiquette (EEMA, 2002).

This thesis shows that spam is an increasing problem for information society citizens. For the senders of spam, getting the message to millions of people is easy and cost-effective, but for the receivers the cost of receiving spam is financial, time-consuming, resource-consuming, possibly offensive or even illegal, and also dangerous for information systems. The problem is recognised by governments who have attempted legislative measures, but these have had little impact because of the combined difficulties of crossing territorial boundaries and of continuously evasive originating addresses. Software developers are attempting to use technology to tackle the problem, but spammers keep one step ahead, for example by adapting subject headings to avoid filters. Filters have difficulty differentiating between legitimate e-

mail and unwanted e-mail, so that while we may reduce our junk we may also reduce our wanted messages.

Putting filter control into the hands of individual users results in an unfair burden, in that there is a cost of time and expertise from the user. Where filter control is outsourced to expert third parties, solving the time and expertise problems, the cost becomes financial. Given the inadequacy of legislation, and the unreliability of technical applications to resolve the problem, there is an unfair burden on information society citizens.

This research has resulted in the conclusion that cooperation between legislation and technology is the most effective way to handle and manage spam, and that therefore a defence in depth should be based on a combination of those two strategies. The thesis reviews and critiques attempts at legislation, self-regulation and technical solutions. It presents a case for an integrated and user-oriented approach, and provides recommendations.

# ACKNOWLEDGEMENTS

First of all I would like to thank my parents Julie and Sotiris Moustakas and my sister Hope Moustakas. There are no words to describe my appreciation, love and respect to them.

During the research I have been fortunate to meet and work with many gifted people, and neither time nor space will permit me to highlight all of them. The research would not have been possible without the assistance and cooperation of academics, IT professionals, legislators and organisations both in the UK and internationally.

Words cannot express my gratitude to and respect for:

Professor Colin Tully (Director of Research, School of Computing Science, Middlesex University), for his continuing support during the whole programme: he was a powerful source of motivation and encouragement, that enlightened the research in critical times;

Dr Penny Duquenoy (my Director of Studies) for being an outstanding supervisor: not only had she an exceptional knowledge in the area of computing ethics but she had also the talent to supervise and guide a research project in a professional and well-structured way;

Mr John Weldon (second supervisor), for his outstanding supervision: his contribution gave a high standard of quality to the project;

the Greek State Scholarships Foundation [http://www.iky.gr], for agreeing to extend the length of the scholarship at Middlesex that I was awarded in 2000 for a masters in e-commerce, to include two additional years for a doctors programme in the area of unsolicited commercial communication (spam);

Professor Terzides Konstantinos (Supervisor of the Greek State Scholarships Foundation), for his overall valuable support during the programme;

the academic staff in the School of Computing Science at Middlesex University during my masters programme in e-commerce (awarded in December 2001), for giving me the necessary educational background and motivation to continue for a doctors programme; and

the academic staff in the Middlesex University Business School during my bachelors programme in business administration (awarded in July 2004), for discussing the problem of spam and recommending different ways and approaches to tackle the problem.

I would like to thank the following organisations and individuals for giving me key opportunities and help:

The University of Illinois at Chicago, for giving me a scholarship to continue part of the research in Chicago during the academic quarter September–November 2004, and specifically

Professor Chandrasekaran Ranganathan, for his valuable feedback and guidance during my academic visit at UIC, and

Mrs Ann Rosi (Assistant Director, Doctoral Programs and Research, College of Business Administration, UIC);

Loyola University of Chicago, for an invitation to address the Loyola Marketing Club on the theme "Unsolicited commercial communication (spam tale): problems and possible solutions" (October 2004), and specifically

Professor Raymond Benton (Professor of Marketing),

Mr David Seuc-Rocher (President, Loyola Marketing Club), and

Mrs Eve (Evanthia) Geroulis (Lecturer, Internet Marketing Class);

the Polytechnic Institute of Viseu, Portugal, for an invitation to give a guest lecture on spam and cyber fraud (February 2005), and specifically

Mrs Ana Branca (Lecturer);

Turku University, Finland, for an invitation to give a guest lecture entitled "Kill spam volume 4: the integrated scenario" in the Department of Information Technology, and specifically

Mr Kai Kimppa (Assistant Professor, Information Systems, Department of Information Technology);

Atlantic Supermarkets SA, Greece, for implementing my e-mail policy and providing valuable feedback for chapter 8 on corporate e-mail policies.

I would finally like to thank:

Jean-Jacques Sahel (Head of International Communications Policy, Department of Trade and Industry);

Philippe Gerard (DG Information Society, European Commission);

Erkki Liikanen (European Commissioner for Enterprise and Information Society);

Phil Jones (UK Data Protection Commissioner, Privacy and Spam);

Professor Dr Michael Walrave (Catholic University of Leuven);

Professor Ifan Shepherd (Professor of GeoBusiness, and Head of the Centre for Transfer Research and Applications, Middlesex University);

Constance Bommelaer (Media Development Department, Prime Minister's Services, France);

Dr Claudia Kalay (Research Manager, School of Computing Science, Middlesex University);

Dr Robert Pleass (Research Manager, School of Computing Science, Middlesex University);

Kerry Gaulton (Research Administrator, School of Computing Science, Middlesex University);

Shelley Milosevich (Social Worker, University of Illinois at Chicago);

Nick Paraskevopoulos (General Manager, NETFORCE Internet Business Services, Athens);

Dr Yaw Busia (Lecturer, School of Computing Science, Middlesex University);

Katrin Tagel.

# CHAPTER 1 INTRODUCTION TO THE RESEARCH AREA

## 1. Introduction

There is no universal definition of spam. In 2002, the Australian National Office for the Information Economy (NOIE) encountered the difficulty in trying to define the term spam when it conducted an extensive review of the spam issue. In its review, NOIE, while recommending further work on a widely recognised and accepted definition, did develop a working definition: it defined spam e-mail as a communication that could not be reasonably assumed to be wanted or expected by a recipient. The above definition is adopted in this research, with terms such as "unwanted" and "unexpected" being replaced by "unsolicited".

The current research investigates unsolicited commercial communication and its impact on individual users, corporations and internet service providers. The objective of the research has been to tackle the problem of spam. The following section discusses the different aspects of spam and explains the different perspectives taken in the research. The current chapter concludes by summarising the key points of the research and its contribution to knowledge.

## 2. The problem

E-mail enables us to share data more easily and efficiently than ever before. It is an efficient method of soliciting customers and selling products. As more consumers gain e-mail addresses, the efficiency of using e-mail as a marketing tool will grow. Although e-mail is a good marketing tool (Chaffey, 2003) it is also a problem for consumers, corporations and internet service providers (International Telecommunication Union, 2003). This is discussed in Chapter 4.

The first task of the research was to find evidence that spam is a problem for consumers. A questionnaire was developed as part of the research and was distributed to two hundred individuals at Brent Cross Shopping Centre in London UK, two hundred individuals in Chicago Illinois, and two hundred on-line e-mail users. The

outcome of the survey showed that individuals believe that spam is a problem (discussed in chapter 3).

While unsolicited commercial e-mail (UCE) serves as a low-cost marketing tool for senders, it poses a serious threat to the privacy of individual internet users (Meade, 2003). The practice of spamming, and in particular the way in which e-mail addresses are collected or sold, raises a number of on-line privacy issues.

The research proves that there is a direct relationship between spam and cyber crime (discussed in Chapter 4). Techniques such as phishing (i.e. creating fake identities using spoofs of well-known domain names, such as ebay and amazon), that fool the user into providing personal information such as financial data, bank account numbers and passwords, have become increasingly sophisticated (Graham, 2002).

A significant proportion of UCE contains fictitious information about the sender, misleading subject lines or performance claims, advertisements for pornographic web sites, software offers for collecting e-mail addresses, fake products or pirated software. Therefore, UCE poses a fundamental threat to e-commerce (Industry Canada, 2005). EU Enterprise Commissioner Erkki Liikanen has said: "Spam undermines consumer confidence, while consumer confidence is a prerequisite for the success of e-commerce and, indeed, for the Information Society" (EU Business, 2005).

UCE also burdens internet service providers (ISPs), who bear much of the cost of providing the infrastructure. Spam consumes resources such as network bandwidth, storage space and computing power, causing significant performance issues for ISPs as well as for their clients. Moreover it creates support overheads for ISPs, who must deal with spam complaints from their customers (OECD Task Force on Spam, 2005).

Lost productivity is another negative effect of spam (Khong, 2004). When employees receive UCE at work, their work time is spent in reading and deleting messages. For organisations, a percentage of labour cost is spent on employee time dealing with junk mails, apart from the additional workload for their data centre and MIS staff (Nucleus Research, 2003). There are other productivity drains as well: there have been

instances of lawsuits as a result of pornographic and other messages circulated via e-mail in the workplace.

Junk e-mail not only costs corporations dearly in precious network resources and employee productivity but also carries with it serious legal liability as well as network security risks.

UCE is also increasingly used as a vehicle for spreading computer viruses and worms. Spam and e-mail-born viruses can no longer be treated as separate problems. More than 98% of computer viruses now arrive via spam, cleverly camouflaged with introductory subject messages like "I love you" or tempting picture attachments (Dearsley, 2004).

Spam, which most frequently takes the form of mass mailing advertisements, is a violation of internet etiquette (also called netiquette), an unofficial code of on-line conduct (JNUG Netiquette, 2005).

A number of conferences have been organised on the topic of spam: they have provided valuable feedback and showed that spam was a serious problem.

The following list was the first attempt to identify and categorise the major stakeholders of spam.

- Senders of spam (corporations, direct marketers).
- Government (produces legislation).
- Intermediaries (ISPs, marketing associations, consumers' privacy associations, lawyers, software/hardware developers).
- Receivers of spam (individuals, enterprises).

## 3. Objectives of the research and contribution to knowledge

The objective of the research is to investigate ways of eliminating UCE. In order to achieve that objective the research first produces evidence that spam is a problem, then introduces the idea of an integrated approach, and finally provides recommendations for both the legal and technical environments.

The approach used in this research reviews and critiques the current attempts at anti-spam legislation, self-regulation and technical solutions. It presents a case for an integrated user-oriented approach, and provides recommendations in both the IT and the legislative areas. The integrated approach will provide organisations with fundamental and practical advice to deal with spam issues and to protect their corporate assets from on-line criminal activities (often known collectively as "cyber-fraud").

The research proposes that neither legislative nor technical measures are sufficient on their own. None of the stakeholder groups can tackle the problem of spam alone. For example, there is no anti-spamming software package that is sufficient by itself to tackle the problem. An e-mail blocking system is only a part of an overall information security effort. Cooperation between the law and IT is the most effective way to combat spam, and therefore an effective solution should be based on combination of the two areas.

This proposed solution – an integration of policy and practice – is the main contribution of this research. The concept of integrating policy and practice is referred to through the rest of this thesis as the "integrated scenario" (i.e. the envisaged outcome of integration).

## 4. Spam stakeholder analysis

After identifying the major spam stakeholders, the next task was to investigate the level of their involvement in the spam problem by conducting a stakeholder analysis. Through this analysis, the major spam stakeholders were identified, as well as their positions and potential roles in the UCE process. More specifically, a table was produced that contains important information about each stakeholder (discussed in Chapter 3). The stakeholder analysis demonstrated more clearly the areas for future investigation, such as legislation, technical anti-spam measures, and corporate e-mail policies.

## 5. Research on anti-spam legislation

Spam has been the most visible e-mail threat, and has reached a point where it creates a major problem for the development of e-commerce and the information society.

According to the International Spam Enforcement Workshop that was held in London in October 2004 (Office of Fair Trading, 2004), it is estimated that 60% of all e-mail messages are spam.

The USA, Australia, Canada and EU member states have all implemented legislation in an attempt to combat UCE. Their statutes feature a wide range of anti-spam measures including labelling requirements, prohibition on using deceptive techniques such as false headers, the creation of do-not-spam lists, and penalties for sending spam.

The most critical debate is about whether to force consumers to ask to be removed from receiving commercial marketing (opt-out) or to force businesses to obtain recipients' consent before sending commercial e-mail marketing (opt-in). While the USA and Japan have adopted an opt-out approach, the EU, Canada and Australia have voted for an opt-in framework. However, because of the difficulty and complexity of the problem, the implementation and enforcement of the law in a global environment is still to be resolved.

This part of the research provides an overview of the various laws relevant to the problem of spam, and compares different anti-spam legislation around the world. It examines the extent to which laws address the problem of spam, and discusses their weaknesses. It compares the EU spam directive as implemented in the UK with the CAN-SPAM Act in the USA. Then it analyses the familiar failures of CAN-SPAM and goes on to make recommendations, mostly that some technical improvements are needed: they include better sender authentication, international legal cooperation, and global harmonisation of spam laws.

## 6. Technical anti-spam solutions

One approach to resolving the problem of spam is to use technology. The stakeholder analysis showed that anti-spam software or hardware solutions are usually developed by ISPs or anti-spam vendors. Technical anti-spam solutions include black/white lists, first- and second-generation technical anti-spam solutions, and Bayesian filtering (discussed in Chapter 7). The research claim on this point is that no anti-spamming software package is 100% effective. The research investigates some of the technical

measures that are available to combat the problem, and provides an evaluation of some common applications. The research suggests that, despite improvements in the performance of anti-spam technologies over the last two years, a technical solution by itself is not enough to tackle the problem of spam.

## 7. Corporate e-mail policies

A result of the stakeholder analysis is to show that organisations are interested in combating lost productivity. One way of doing this is to have an e-mail policy (discussed in Chapter 8). The research claim on this point is that the level of spam can be decreased within the organisation through the development of a corporate e-mail policy and through putting appropriate security controls in place to protect corporate information.

This research explores the risks involved with employee e-mail use, discusses a framework for governing an effective e-mail policy, and provides organisations with a comprehensive view of e-mail security through the development of corporate e-mail policies. Many organisations are looking for ways of reducing risks by controlling employee use of e-mail through the implementation of employee Acceptable Use Policies (AUPs) and enforcing these by implementing technical solutions.

# CHAPTER 2 LITERATURE REVIEW

This chapter reports on the situation regarding spam during the period of this research. The literature and reports showed there are many sides to the problem. As the research progressed different stakeholders were identified, and investigated separately.

## 1. Introduction

It was briefly mentioned in Chapter 1 that the increase of global internet and e-mail as the new means of communication enables us to share information more easily and efficiently than before. An International Data Corporation (IDC) report estimates that e-mail messages sent per year will increase from 9.7 billion in 2000 to 35 billion in 2006 (International Data Corporation, 2000). According to the Gartner Group, e-mail messaging has increased at a compound annual growth rate of 40% since 1981 (Gartner Group, 2001). However, if the increase in e-mail use is matched by an increase in the level of spam, it creates a variety of problems for consumers, businesses, ISPs and legitimate marketers (Metchis, 2003).

## 2. Why spam is a problem

In June 1997 the Federal Trade Commission (FTC) organised a Workshop on Consumer Privacy, which marked the beginning of a focused discussion of the problems associated with UCE (Centre for Democratic Technology, 2004). The FTC has recently stated that spam is one of the most difficult consumer protection problems the US government has ever faced (Federal Trade Commission, 2005). The extremely low cost of sending e-mail makes it a very appealing marketing channel. However, low cost when combined with anonymity makes spam an ideal vehicle for conducting illegal activities. A 2003 FTC staff survey revealed that two-thirds of spam in its sample contained "facial indications of falsity" which means that e-mail appears to be something else from what it really is (Federal Trade Commission, 2003).

In 2003 internet subscribers worldwide were unwittingly paying an estimated €10 billion a year in connection costs just to receive junk e-mails, according to a study undertaken for the European Commission (European Commission, 2003). The study provided detailed information on the junk mail phenomenon in the USA and the EU,

and formed part of the Commission's efforts to ensure that the development of the internet and e-commerce did not undermine European rules on internet privacy and data protection. The following diagram pictures the level of spam within the member states of EU in 2002 (Figure 1).

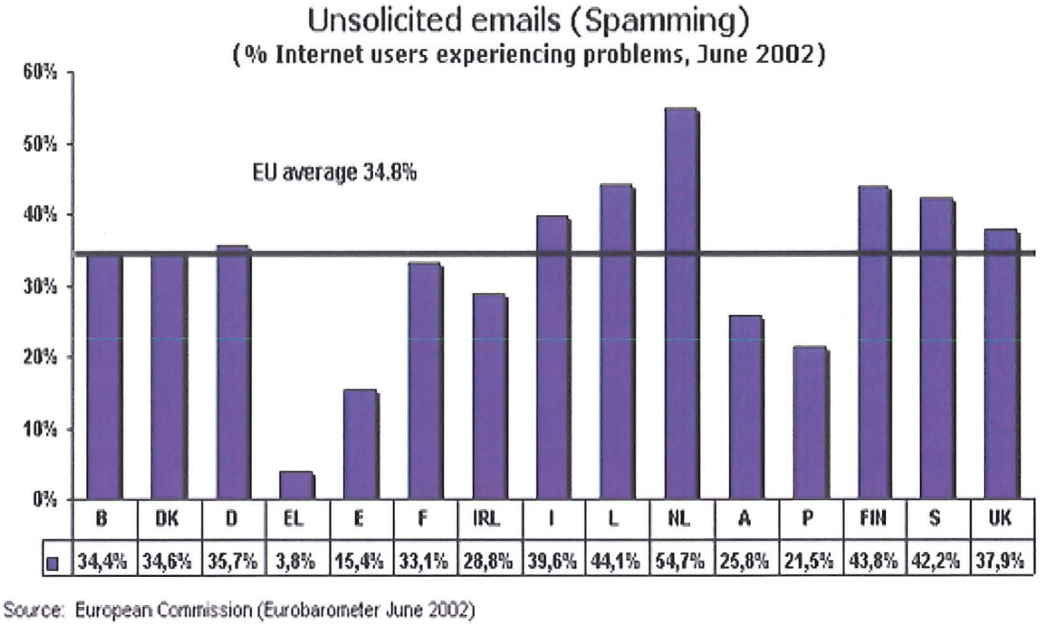



***Figure 1 – The level of spam in the EU (2002)***

Spam is a major problem for developed countries, but perhaps is even worse for developing and less developed countries, where, because of limited available internet resources, many users rely on free web-based e-mail services with limits on free storage, which are particularly targeted by spammers (Horton, 2004).

Spam cannot be tackled easily. Senders of spam routinely investigate new and innovative ways to avoid having their e-mails blocked. Blocking spam by using technology can be difficult because what is spam to one individual or organisation is a legitimate message to another.

Spam impinges on the privacy of individual internet users. It can also cost users in terms of the time spent reading and deleting the messages, as well as in a traditional economic sense where users pay time-based connection fees. Spam, which most frequently takes the form of mass mailing advertisements, is a violation of internet etiquette (Koppanyi, 2003).

The cost incurred by individuals to protect themselves from unwanted e-mail messages is significant. The privacy cost includes the purchase of anti-spam software filters for stopping junk mail, avoiding identity theft and protecting privacy on the internet. A privacy-sensitive family could spend between $200 and $300 and many hours annually to protect their privacy (Gellman, 2002).

Second, spam burdens ISPs, who bear much more of the cost of providing the infrastructure than the sender does, and who frustrate their customers who have to suffer poorer performance levels (Cerf, 2002). Moreover it creates support overheads for ISPs who must deal with spam complaints from their customers. In the case of America Online Inc (AOL) v Prime Data Worldnet Systems Inc, AOL attempted to block Kentucky-based spammer Prime Data Worldnet Systems and its proprietor, Vernon Hale, from sending spam to AOL members. The plaintiff claimed and won direct computer costs of 78/1000 of a cent per message from defendants Prime Data Worldnet Systems Inc (AOL Legal Department, 2003).

Lost productivity is another negative effect of spam. According to the 2004 National Technology Readiness Survey, an annual survey that tracks US consumers' technology opinions and behaviours, online users in the USA spend an average of three minutes deleting spam each day they check e-mail. Aggregating their usage across the 169.4 million online adults in the United States, that equals 22.9 million hours a week, or $21.58 billion annually when based on the average working wage (National Technology Readiness Survey, 2004).

The cumulative costs add up quickly when e-mail users spend a few minutes per day dealing with and disposing of spam. Labour costs increase because employees are spending time deleting junk e-mail, not to mention the diversion of attention of data centre and information systems staff.

There are other productivity drains as well: on the legal front, there have been many instances of lawsuits as a result of pornographic and other messages circulated via e-mail in the workplace.

Spam also poses a threat to consumer confidence in e-commerce (EuroUnion, 2003). That is because a significant proportion of spam contains fictitious information about

the sender, misleading subject lines and extravagant earnings or performance claims about chain letters, pyramid schemes, advertisements for pornographic web sites, offers of software for collecting e-mail addresses, cheap quality products or pirated software.

Finally, one of the biggest problems associated with spam is that of viruses. According to Dearsley (2004) 98% of computer viruses arrive via spam, cleverly camouflaged with introductory messages like "I love you" or tempting picture attachments of Britney Spears, Madonna or Anna Kournikova. The Melissa virus was significant in that it was the first major example of spam effectively hijacking the users' computers. This type of malicious program code can take the form of a Trojan horse and may cause harm to the e-mail recipient's computer. It can get control of the recipient's computer and do its chosen form of damage, such as ruining the file allocation table on the hard disk.

## 3. Initiatives to address the problem of spam

This section provides an overview of the initiatives by government, ISPs and technical anti-spam vendors to address the problems of spam, and describes the broad position of each in relation to the sending of spam. These are categorised as follows.

- Spammers – defenders of spam.
- Internet service providers (ISPs).
- Government – legislation.
- Technical anti-spam vendors.
- Marketing associations and ISP associations.

### 3.1 Spammers – defenders of spam

It has been argued that the sending of junk promotional e-mail represents a form of free speech (Centre for Democratic Technology, 2001). The difficult question is how to balance the right of commercial free speech with the privacy right. Some of the senders of spam argue that spam is not different from conventional paper junk mail. On the other hand, the opponents of spam claim that it consumes resources from ISPs and consumers. The major difference between electronic mail and paper junk mail is that the cost per copy of sending junk e-mails is much lower. For instance, one direct

marketer specialising in spam charged his clients a small fee of about $500 to send out several million messages, and claimed that "It's just as cost-effective to send to six million e-mail addresses as to one million, so why bother being selective?".

Those who defend spam claim that, while it imposes some costs on its recipients, those costs are trivial, and that many users enjoy and benefit from this form of advertising (Spinello, 1999). Unsolicited e-mailing does not mean necessarily that the e-mails are unwanted by everyone. Spam represents an efficient and inexpensive way to advertise worthwhile products and makes it easier for small enterprises to advertise their products in a cost-effective way. Similarly, the chance to advertise products and services to millions of customers represents a significant economic opportunity for small and medium enterprises and it should not be undermined by restrictive regulations (Chaffey, 2003). Finally the proponents of spam support methods of collecting e-mail addresses. They believe they have the right to gather e-mail addresses from various sources (newsgroups, online directories, web pages) and use them for sending commercial e-mails. They claim that e-mail addresses are as public as phone numbers. They claim that if someone does not want to receive junk e-mail he should not place his address anywhere that is publicly accessible.

## 3.2 Internet service providers (ISPs)

No matter how the internet may be transformed and what it may mean to people, it is likely that there will be a continued need for the provision of access services. Internet service providers have become a critical component of the commercial internet, providing customers with internet access, web hosting services, e-commerce technologies and e-mail access. The stakeholders most able to tackle the problem of spam are the ISPs. According to the Electronic Commerce Regulations 2002 (EU Directive 2002/58/EC, 2002), ISPs are "mere conduits" and as a result are not liable for the content of information they transmit through their networks. In general they are not expected to monitor every single e-mail.

An intermediary, such as an ISP, who provides services related to internet transactions, runs two separate liability risks. An ISPs's action or inaction in the course of providing a service may cause loss to a communicating user or third party. In most jurisdictions the law will imply that the ISP must take reasonable care in the

provision of services to its user. Thus, the ISP would be liable for failing to process an outgoing or incoming communication, but only if the failure should have been avoided. In relation to spam, if the ISP guarantees a spam-free e-mail service, then it is liable to its customers in the case that they receive unsolicited e-mails. An ISP might be held responsible for the content of the information it has transmitted, either being forced to pay compensation to the person aggrieved by the content, or even for committing a criminal offence. If the unsolicited e-mail communication contains defamatory statements or offensive material, ISPs might be liable toward its customers.

Several ISPs offer newsgroup services to users. There are legal cases such as Stratton Oakmont Inc v Prodigy Services Co (Stratton Oakmont Inc v Prodigy Services Co, 1995) where the ISP was sued because it was responsible for filtering the content of the groups. If the ISP held itself out to the public and its members as controlling the content of its computer bulletin boards then e-mails should be checked before they are published. In that case, if an e-mail message contains a defamatory statement and the ISP receives a notice about the situation, immediate action needs to be taken. Dubious newsgroups and forums need to be controlled regularly by the ISP, and each of its members should provide full name and address before entering a forum (i.e. not allowing anonymous guest members).

Since the introduction of e-mail, addresses (other than business addresses) are deemed to be personal information (Data Protection Act, 1998). This legislation imposes restrictions and obligations on how addresses and other personal information are collected, used and disclosed in the course of commercial activity by ISPs. The law also creates an obligation for those firms and others who store electronic mail addresses to provide appropriate security for this personal information. Firms buying, selling, leasing or bartering electronic mailing lists would be subject to the provisions of the legislation, if these transactions take place over provincial and national borders.

## 3.3 Government – legislation

### 3.3.1 Introduction

The government provides legislation to secure the e-commerce environment (Wall, 2004). There are national laws such as the Canadian Code of Practice for Consumer

Protection in E-Commerce, the USA Act of 2000 for Unsolicited Commercial Electronic (UCE) Mail, or set by other legislative bodies such as European Union (EU Directive 2002/58/EC, 2002). The following sections describe the laws in selected countries pertaining during the time of research.

### 3.3.2 EU legislation

In July 2002 the European Parliament and Council voted (EU Directive 2002/58/EC, 2002) to ban spam. That meant that people would have to opt in or ask to receive commercial e-mail. The Directive had a small positive impact. Many people were sceptical about the effectiveness of the legislation since much of the spam originated from outside the EU. Below is a part of the Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector.

> (40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them.
>
> (41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC.
>
> (43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.
>
> (44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments.

One of the main changes in relation to e-mail was the shift to an opt-in regime. Under Article 13 of the Directive the use of e-mail and SMS (text messages to mobile phones) for direct marketing is only to be allowed in respect of subscribers who have given their prior explicit consent. This puts e-mail marketing on the same footing as unsolicited faxing and automated telephone systems. The Directive makes an exception where there is an existing customer relationship and the supplier has obtained the customer's details in the context of a sale of goods or services. In this

case the supplier may use the customer's details for the purpose of direct marketing in relation to its own similar goods or services.

The Directive states that the customer must be clearly and distinctively given the opportunity to object free of charge and in an easy manner to the use of the e-mail address when it is collected, and on the occasion of each message in the case that the customer has not initially refused such use. This exception leaves open to interpretation whether goods or services advertised are similar to those previously purchased. Moreover it appears from the wording that the exception only applies where there has been an actual sale rather than, for example, an enquiry. It also appears that only the party that obtained the details can use them: so, for example, a manufacturer could not e-mail its customers where the e-mail address was obtained by a retailer. The Directive also prohibits sending direct marketing e-mails which disguise or conceal the identity of the sender or are without a valid address to which the recipient may send a request that such communications cease.

According to the Data Protection Act (Data Protection Act, 1998) and the Directive on Privacy and Electronic Communications (EU Directive 2002/58/EC, 2002), it is illegal to send e-mail to people who were not expecting it, if that e-mail could be regarded as commercial. The effectiveness of the EU Directive is minimal since most spam originates from outside the EU. Also there could be a difficulty when a consumer is interested in a specific product or service and wants to request information from relevant companies. Although consumers are generally aware of the larger companies, they are unlikely to know about many of the small and medium-size companies who offer similar products/services at competitive prices.

In August 2003, marketing managers at one hundred technology firms took part in a survey to investigate the impact of the new e-mail marketing law. The survey was commissioned by e-marketing communications agency StoneShot. The law would mean that commercial e-mail could only be sent to people who have chosen to receive it. Widely used opt-out lists (where people are added automatically and must unsubscribe to stop further mailings) were banned. Although all companies polled were using e-mail for marketing and had substantial mailing lists, only 30% considered themselves fully aware of the law and only 37% had an opt-in list. 21% had no clear policy on whether their list was opt-in or opt-out. Companies were asked

whether they knew about the law change, and an alarming 21% said they knew nothing about it. A further 49% said they had heard something about it, but only 30% said they were fully aware of legislation. While the law is complicated, companies depending on e-mail marketing to generate and retain business had to act to ensure that their business will not be adversely affected by the legislation.

### 3.3.3 The position in the USA

In order to analyse the environment before the implementation of the Unsolicited Commercial Electronic (UCE) Mail Act of 2000, different legal cases were selected relevant to spam. Two distinctive cases are:

- BiblioTech Ltd (UK ISP) v Sam Khuri/Benchmark (2000), and
- AOL v Web Communications (2002).

The actions brought by Bibliotech and AOL were not for any offence of spamming, since such an offence did not exist as yet in the USA. The actions were brought on the basis that Khuri and Web Communications were tying up their servers, which cost money and reduced the quality of service to Bibliotech's and AOL's customers.

Bibliotech stated in press releases (Hamiltons Solicitors, 2003) that one of the principal factors that prompted them into bringing action was that Khuri was allegedly running a scam, offering cheap toner cartridges but failing to deliver once money had been handed over. Web Communications, despite demands by AOL that they cease sending their unsolicited e-mail, refused to stop mass mailings and adopted deceptive techniques designed to frustrate AOL's ability to detect and filter these e-mail messages. Among other tactics employed, defendants forged aol.com within their e-mail messages so that the messages falsely appeared to originate from an AOL member. In addition to these practices, defendants operated sites on the World Wide Web using the AOL trademark and service mark as part of several of the defendant's domain names. It was claimed that the defendant's indiscriminate mass mailings and deceptive practices caused serious and irreparable injury to AOL by impairing the functioning of AOL's e-mail system and harming AOL's business reputation and goodwill among its members.

In the USA various anti-spamming legislative measures at both federal and state levels have been introduced to stop spam. California, Nevada, Washington, Massachusetts and Connecticut have already passed such legislation. In California, in addition to criminal liability for hacking and using the domain name of another (up to a year's imprisonment), e-mail service providers can recover their actual monetary loss or liquidated damages of $50 per e-mail (maximum $25,000 a day). In Washington, recipients can collect $500 in damages for each piece of spam. These concerns have led large service providers (notably AOL) to bring successful court cases against spammers in the USA. Spammers in the USA run the risk of being sued by ISPs, who have used the following laws to uphold their case:

- the Computer Fraud and Abuse Act;
- the Lanham Act for false designation of origin, and
- various State Computer Crimes Acts.

The Unsolicited Commercial Electronic (UCE) Mail Act of 2000, also called the Anti-SPAM Act, made more progress than any previous attempt at legislation and also won approval from the US House of Representatives in July 2000. On 23 May 2001, however, a Washington House committee scaled back legislation that aimed to curb junk e-mail, cutting out provisions that would allow consumers to sue companies that ignore requests to be taken off their mailing lists. The House Judiciary Committee also added a measure that would require pornographic messages to be labelled as such, allowing consumers to delete the messages without opening them if they so desired. The Bill passed on a voice vote after lengthy debate. The courts ruled that at least two laws against spam were unconstitutional in Washington and California because they were "unduly restrictive and burdensome". Also advertisers in Colorado required labelling their messages as advertising by placing the letters "ADV" in the subject line, thus making messages easy to delete.

### 3.3.4 The Canadian code of practice for consumer protection in e-commerce

Distribution of unsolicited promotional and product information, in print form or over electronic networks, is not illegal nor is it regulated in Canada. In the same way, advertising, except in the Canadian Broadcasting System, is generally not federally regulated. There are, however, specific provisions in various laws dealing with such

things as tobacco advertising or misleading advertising in the Competition Act (Competition Act Canada, 1985). Spam is also considered a form of expression and, as such, any attempt by the government to control it, regardless of the means, would have to be consistent with section 2 of the Charter of Rights and Freedoms (Canadian Charter of Rights and Freedoms, 1982). Internet service providers are subject to the same laws and regulations as most other businesses, and there are no special rules for the internet service industry. Unlike the telephone companies, ISPs are generally not subject to regulation under the Telecommunications Act because they are not considered to be facilities-based common carriers.

The Working Group on Electronic Commerce and Consumers developed the Canadian Code of Practice for Consumer Protection in Electronic Commerce, based on the Principles of Consumer Protection in Electronic Commerce. The Code is consistent with the Organisation for Economic Cooperation and Development's Guidelines for Consumer Protection in the Context of Electronic Commerce. The Code was also the subject of extensive consultation. The Working Group approved the Code in principle as a model for effective consumer protection in electronic commerce, and recognised that the Code needs to be systematically assessed through a pilot testing process. From January to March 2003, the Code was used for pilot testing by a number of industry sectors. The Code was then reviewed and revised (as necessary) by the E-Commerce Leaders Code Review Committee from April to June 2003. The reviewed and revised version of the Code was then available for endorsement by all interested parties from July to September 2003. The revised Code was published in the autumn of 2003.

The Act prohibits false or misleading representations to the public; it focuses primarily on the application of the Act to commercial web sites and marketing strategies using e-mail. Principle 4 refers to online privacy, and principle 7 reviews spam.

**Principle 4: Online privacy**

[4.4] Vendors shall not disclose personal health information to affiliates or third parties for purposes other than the transactions unless specifically and expressly authorised by consumers in advance, through a clearly worded opt-in process. When seeking consumers' express consent to disclose the information, vendors shall list the information to be disclosed, all uses to which it may be put and all parties to whom it may be disclosed.

[4.5] Vendors shall not, as a condition of sale, require consumers to consent to the collection, use or disclosure of personal information beyond that necessary to complete the sale.

**Principle 7: Unsolicited e-mail**

[7.1] Vendors shall not transmit marketing e-mail to consumers without their consent, except when vendors have an existing relationship with them. An existing relationship is not established by consumers simply visiting, browsing or searching vendors' Web sites.

[7.2] Any marketing e-mail messages vendors send shall prominently display a return e-mail address and shall provide in plain language a simple procedure by which consumers can notify vendors that they do not wish to receive such messages.

According to a report by the Canadian government in 2002, they believed that an appropriate mix of policies and laws, consumer awareness, responsible internet industry stakeholders and technological solutions is the best and most appropriate way to deal with behaviour in the new and evolving on-line environment. At that time, the Canadian government believed that they had the right mix but would continue to monitor developments and consider changes if required (Industry Canada, 1997). The Canadian government was giving priority to a combined approach where the various stakeholders would work together to tackle the spam problem. However, no further information was given on how this mix of policies and laws could work together.

### 3.3.5 Spam-blocking law proposed in Japan

The country's largest opposition party, the Democratic Party of Japan, brought forward a bill in 2001 forbidding the practice of spamming to parliament (IDG News Service, 2001). The bill consists of three parts.

- Senders are obliged to state this is an advertisement when sending non-requested e-mail.
- Senders are never allowed to send e-mail to recipients who have informed senders by phone or e-mail that they refuse e-mail from them.
- Telecommunication carriers can refuse e-mail from spammers when it might cause system problems.

In the bill, spam is defined as mail that is sent for vendors' advertising purposes without recipients' consent or request. E-mail senders are obligated to disclose their name, address and e-mail address and to inform recipients that they have the right to refuse such mail (Miyake, 2001).

## 3.4 Technical approaches to blocking

Another approach used to prevent spam is the technical one. The following sections describe various technical methods for handling spam.

### 3.4.1 Real-time blocking lists

One of the ways of preventing spam is to use lists of known spammers and to discard messages originating from those addresses or domains. One such offering is the MAPS Realtime Blackhole List (Realtime Blackhole List, 2002), or RBL, a free service run by the Mail Abuse Prevention System, a non-profit organisation dedicated to making the internet as spam-free as possible. The RBL is a global clearing-house of information about systems where spam originates and systems that provide support services to spammers (Realtime Blackhole List, 2002). The idea behind the RBL is that a subscriber's e-mail server will consult the MAPS database as each piece of mail is received, and check the sender against the list. If the message comes from a site on the list, it can be discarded, or at least marked as probable spam, before it hits the user's mailbox. Use of a blocking list can give rise to only one response – to block reception. The technique cannot differentiate between individual e-mails; all e-mail from the named source will be blocked. However, for some sources of "dark spam", e.g. known pornographic spammers, blocking is typically the best approach. The problem with the block list approach is that the originating address of a message can be spoofed. The spammer can easily make e-mails look as though they are originating from legitimate addresses.

### 3.4.2 Content filtering technologies

In order to deal with the problem of filtering incoming spam based on originating addresses, and to scan inbound and outbound e-mail for confidential information, some sort of keyword examination of the message content is needed. The difficulty is to decide which words are offensive. Elron, an anti-spam software company, has partnered with the publishers of the Oxford English Dictionary to develop a list of offensive terms (Information Security Magazine, 2000). Content Technologies' MailSweeper and MIMESweeper were amongst the first major anti-spam products aimed at the corporate market (ClearSwift, 2003). MailSweeper was designed to integrate with SMTP, Microsoft Exchange and Lotus Domino mail servers to provide

e-mail content protection, including keyword filtering of incoming and outgoing messages, to provide protection from viruses in incoming and outgoing messages via integration with third-party virus scanners, and to add legal disclaimers to outgoing messages.

Like the analysis of web pages, using simple keyword searches to analyse the content of e-mail may cause many false positive hits. Elron offered Command-View Message Inspector, a product using full-text analysis technologies to scan e-mail for inappropriate content. According to Elron, these techniques determine the context of a word or phrase within a message before deeming the message to be a security threat, objectionable or spam. These technologies take into account factors such as the relative position of words and the number of times each word appears. Message Inspector allowed the filtering of inbound and outbound e-mail, FTP and Usenet traffic for objectionable and confidential information.

MailWasher (MailWasher, 2001a) uses an algorithm to determine the best route to send bounced messages back (from, reply to, return path) and returned them via the ISP's postmaster, so that it looks exactly as though they had come from the receivers' ISP and not from the recipients' e-mail address. If the spammer used a fake address, then the bounced message would itself be bounced back to the postmaster and the recipient would not receive the bounced e-mail. The bounced messages look exactly like returned mail messages that would be received if an e-mail had been sent to a wrong address.

The Brightmail (Brightmail Inc, 2001) anti-virus/spam software, Solution Suite 4.0, offered ISPs a spam and virus filtering solution. The software consisted of real-time round-the-clock analysis, automated filtering that was scalable to extremely large mail volumes, and software compatible with a wide variety of e-mail platforms. The Probe Network was a set of dedicated e-mail accounts, which served continuously as an early warning system for the detection of spam and viruses. With a statistical reach of around 150 million mailboxes, the Probe Network included special probe accounts disguised as regular e-mail addresses, allowing Brightmail to catch and analyse spam attacks in their early stages. The Probe Network delivered the latest spam attacks to anti-spam technicians at the Brightmail Logistics and Operations Centre (BLOC), where technicians evaluated them and created customised rules to disable each attack.

These rules were instantly transmitted to Brightmail Servers at participating ISP and Active Server Pages (ASP) sites, where they were immediately put into service. Additionally, BLOC technicians were receiving up-to-the-minute anti-virus definitions and engines from the Symantec Security Response Centre. By the time spam was poised to invade a user's inbox, the Probe Network had discovered it and had prepared rules to block it. The spam was blocked before it could reach the inbox. As e-mail was intercepted from the internet by the Probe Network, it was instantly forwarded for analysis and evaluation by BLOC technicians, who then issued rules to filter the spam. These rules were immediately transmitted to Brightmail Servers at customer sites. System administrators could configure the server to redirect the spam e-mail to a special storage area, where users could easily access and review the messages, using a web-based interface.

ISPs deal with spam in a variety of ways, including automatic filtering technologies, as well as customer-controlled filtering services. In 2002 Microsoft announced that its MSN Hotmail subscribers would be limited to sending only one hundred messages per day, in an effort to prevent spammers from using Hotmail to spread spam (Boston internet.com, 2002). This position was withdrawn a year later because of public demand and competition with other free webmail services. Microsoft now relies on filtering technology. It filters all messages twice, first through its e-mail servers and then at the subscriber end, based on the subscriber's own designation of previous messages as junk.

### 3.4.3 False positives

Anti-spam software packages tend to decide on behalf of users if a message is spam, often resulting in "false positives". A false positive occurs when e-mail is incorrectly categorised as spam and thus does not reach the inbox folder of the recipient. In January 2003 AT&T WorldNet unsuccessfully tried to use a reverse DNS lookup to block spam (CNET News, 2003). ISP servers were programmed to relate an incoming e-mail's originating address to a valid domain name or web address by looking it up in a DNS database; if not there, the message was dropped. However, that approach failed, as too many legitimate e-mails were dropped.

Additionally there were several cases where ISPs incorrectly blocked legitimate personal communications as unwanted e-mail. Legitimate messages were wrongly tagged as junk mail: half went to junk-mail folders and half were not delivered. The real-time blackhole list defines spam not by scanning the content of the e-mail but is based on the names of the servers that e-mail passes through. That may lead to a number of false positives, since organisations and institutions from BT Open-world and Oxford University have discovered that their users cannot send legitimate e-mails, because these institutions have been placed on an anti-spam blacklist. This black list is not valid since a spammer can produce a spoof e-mail looking as though it originated from Oxford University.

In 2003 the magazine ***NetworkWorldFusion*** tested sixteen anti-spam packages on a live production network to check who could solve better the spam problem (NetworkWorldFusion, 2003). Each anti-spam product received two scores. The first score, accuracy, measures how well the filter identified spam. A perfect score would be 100%. The second score is the false positive rate, the ability of the filter to make sure that non-spam messages do not get tagged as spam. A perfect false positive rate would be 0%.

## 3.5 Marketing and ISP associations

Associations of direct marketers in Europe and America also attempt to control their members' behaviour online. However, self-regulation by such bodies is ineffective, as spammers may not be members of the associations. In 2002, the Canadian Marketing Association (Canadian Marketing Association, 2002) established for its members a code and guidelines dealing with internet use for the distribution of promotional materials. Under this code, consumers must be given the opportunity of opting out of any further communication from the marketer. The Canadian Association of Internet Providers (Canadian Association of Internet Providers, 2002) also developed a voluntary code based on the best practices of its membership. Competing for subscribers, ISPs are free to establish their own acceptable use policies and to enforce them through their terms of service agreements. According to CAIP, the vast majority of ISPs prohibit the use of their networks for bulk electronic mailing and reserve the right to terminate the account of any subscriber who indulges in such activities.

Another marketing association is the Direct Marketing Association (Direct Marketing Association, 2002) which is the core trade organisation for all companies involved in direct marketing in the UK and is a member of the International Federation of Direct Marketing Associations and the Federation of European Marketing Associations. The Direct Marketing Association has launched an E-mail Preference Service with a special web site (http://www.dmaconsumers.org/emps.html) where consumers and businesses can register their e-mail addresses to opt out on receiving unsolicited e-mail. Paragraph 5.2.11 of the DMA E-Commerce Code provides that unsolicited e-mail must be clearly identifiable and that members must not send random, untargeted commercial e-mail (spam). Members must use appropriate e-mail preference services and must not send e-mail communications to individuals who have registered an objection to receiving such communications. Finally UCE must include a mechanism for the consumer to register an objection to receiving further unsolicited communication. All DMA members must also comply with a number of general obligations, including disciplinary action resulting from a breach of either the DMA E-Commerce Code or the main DMA Code of Practice.

# CHAPTER 3 METHODOLOGY

## 1. Introduction

This chapter discusses the methodologies used during the research. A combination of qualitative and quantitative methodologies was used. Such a combination (Greene, 1988) has become increasingly popular since it combines the strengths of both approaches: qualitative and quantitative methods are viewed as complementary rather than as rival approaches (Maanen, 1984).

At the beginning of the research the development of a technical anti-spam filter was considered. That was not attempted, first because it was not clear that technical innovations were possible beyond what the ISPs and vendors had already achieved, and second because the timescale of the research would not have permitted adequate evaluation of the performance of a new filter mechanism.

During the research, interviews were conducted with experts in the area of spam. The interviews served a number of purposes.

- Contribute to the design of the open survey questionnaire, which would assist in the formulation of the research hypotheses.
- Contribute to the development of definitions.
- Contribute to the evaluation of hypotheses. For example, interviews with legal experts in the EU helped confirm the research hypothesis that legislation itself is not sufficient to tackle the problem.
- Provide primary data (expert opinion).

All interview notes have been retained for future reference.

In addition to the primary data described above, the following pieces of legislation constituted essential secondary data.

- EU Directive - 2002/58/EC, 2002

  Until July 2002, some EU member states followed an opt-in approach while others used opt-out. In July 2002, the European Parliament and Council voted to

ban spam. Since that date all EU citizens had to opt in or specifically place a request to receive commercial e-mail.

- Can-Spam Act 2003

  The US Can-Spam Act 2003 was signed by the President on 16 December 2003, and took effect on 1 January 2004. The purpose of the Act was to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the internet. The Act represented a compromise between the various spam stakeholders and allowed e-mail marketers to send UCE until consumers opted out from receiving future messages. It also required e-mail marketers to identify UCE as advertisements, as well as to include warning labels on any UCE that contained sexual material. The new legislation was gradually enforced in all the US states and it overrode state laws set by some states.

- Australian Spam Act 2003

  In December 2003, the Australian government introduced legislation which banned commercial and private spam and the harvesting of e-mail addresses. The legislation modified the behaviour of spammers and forced them to leave the jurisdiction. It aggressively required opting in and banned tools for harvesting addresses. Because the Australian Spam Act was significantly important for my research and the development of my ideas for the integrated policy and practice, and since it sent a powerful message to spammers that sending unsolicited electronic junk mail would no longer be tolerated in Australia, this piece of legislation will be quoted frequently in the thesis.

  Court action was taken against an alleged global spammer in the Federal Court in Perth in the matter of Australian Communications and Media Authority v. Clarity1 Pty Ltd and Wayne Robert Mansfield (Federal Court of Australia, 2006). The spammer was found liable, resulting in a fine of A$5.5m (£2.2.m).

The following sections of this chapter review the range of methods that were employed.

- Section 2: determine the scope of the problem.
- Section 3: the open survey questionnaire.

- Section 4: stakeholder analysis.
- Section 5: survey of anti-spam legislation.
- Section 6: technical anti-spam approaches.
- Section 7: corporate anti-spam policies.

## 2. Defining the problem of spam

One of the first objectives of the research was to confirm whether spam was a problem and to analyse how users react to spam. In order to answer that question the following steps were followed.

- Select secondary resources and relevant literature in the area of spam. First initiatives from governments were selected and analysed.
- Conduct an open survey entitled "How users react to spam" with people at Brent Cross Shopping Centre in North London.
- Conduct an on-line survey in cooperation with a Greek ISP, Netforce Ltd, in Athens.

The surveys provided feedback on the different types of spam and the kinds of spam which confront internet users. This part of the research also demonstrated that there is a direct relationship between spam and cyber-crime/phishing. In order to extract accurate feedback, both the on-line and the paper-based surveys included similar questions (Dillman, 2000). The design of the questionnaire will be discussed in the next section.

The second approach was to conduct interviews with IT specialists in the area of spam from ISPs and anti-spam software companies, to find out to what extent companies consider spam a threat to the development of the information society. Interviews are an attractive proposition for the researcher. They do not involve special technology or complex equipment in order to collect the information, except for a notepad and a tape recorder. Though there are similarities between a conversation and an interview, interviews involve a set of assumptions and understandings about the situation which are not associated with a casual conversation (Denscombe, 2000).

## 3. The questionnaire (open survey)

There are many issues that need to be considered in questionnaire design in order to maximise the responses and also to be confident about the reliability of the method (Somekh, 2005). The development of a questionnaire represented a good method of gaining information (Foddy, 1994) about what users think about spam. The questionnaire was distributed to two hundred on-line e-mail users, two hundred individuals at Brent Cross Shopping Centre in London UK, and two hundred individuals in Chicago Illinois.

The online version of the questionnaire was filled in electronically and data entry was automated. Additionally the cost of the online version of the questionnaire was low. However this version introduced a bias since it excluded members with no internet access. For that reason the questionnaire was distributed to individuals at Brent Cross Shopping Centre in London.

Conducting an open survey with the public gave the opportunity to investigate different views of the effect of spam and to establish the extent of the problem. A good questionnaire is quick and easy to fill out. That had to be borne in mind when designing the questionnaire. The same questionnaire was also given to Americans in Chicago during my academic visit to the USA. Some of the questions, such as the names of ISPs or the webmail services, were slightly different so as to be more appropriate for the American public (BT was replaced by AOL, Yahoo.co.uk was replaced by AOL webmail).

According to Covert (1977), the first stage should be to identify the objectives of the survey as well as what questions will be included in the questionnaire. The final number of questions was twelve. Sheatsley (1983) suggests giving a brief introduction at the beginning of the questionnaire explaining the reasons for the survey; that recommendation was followed. The second step was to categorise the questions in groups: the main categories of the questionnaire were finally determined as follows.

**A) About you**

1. Current location
2. Gender
3. Age group

**B) Your access to the internet**

1. Where do you access the internet?
2. What type of internet connection do you have?
3. What internet service provider do you use to access the web?
4. Have you set up an e-mail account with this provider?
5. Which web-based service do you use?

**C) Your e-mail + unsolicited commercial communication**

1. How many spam e-mails do you get on average per day using your ISP's e-mail account?
2. How do you consider spam?
3. Have you got anti-spamming software running on your PC?
4. If you use a web-mail service, how many spam e-mails do you get per day?

**D) Your views**

1. What are your actions in response to spam?
2. Would you be willing to pay an additional fee to your ISP if it provided the guarantee for a spam-free e-mail service?
3. Who do you think, from the following stakeholders, is the most appropriate to handle spam?

In consultation with Professor Ifan Shepherd (Head of the Centre for Transfer Research and Applications, Middlesex University Business School) a number of changes were made in the structure of the questionnaire.

- Section A, "About you", was moved to section D, because it is not appropriate to ask personal questions at the beginning of a questionnaire.
- Most of the questions appeared to allow multiple responses. That should therefore be stated, with "tick one box only" stated otherwise.
- Because of the previous point, several questions needed revision, for example: QB4 should allow for multiple providers if listed in QB3; QC3 should similarly allow for multiple PCs if listed in QB1. As a result QB1 was dropped as a question.
- Some rearrangement of questions would be beneficial. For example, QC2 ("How do you consider spam") is an attitudinal question and should be moved to section D ("Your views"). Also, response c ("I don't think it's important") in

QD2 ("Would you be willing to pay an additional fee to your ISP if it provides the guarantee for a spam-free e-mail service") properly belongs with QC2. The response "I don't think it's important" could be replaced with "Don't know" or "Undecided".

- In QD3 ("Who do you think, from the following stakeholders, is the most appropriate to handle spam?") the respondent may not know what the word "stakeholder" means. For that reason "stakeholder" was removed from this question.

As a result the structure of the questionnaire was updated as follows.

**A) Your access to the internet**

1. What type of internet connection do you have?
2. What internet service provider do you use to access the web?
3. Have you set up an e-mail account with this provider?
4. Which web e-mail service do you use?

**B) Your e-mail + unsolicited commercial communication**

1. How many unsolicited e-mails do you get on average per day using your ISP's e-mail account?
2. Have you got anti-spamming software running on your PC?
3. If you use a web-mail service, how many unsolicited e-mails do you get per day?

**C) Your views**

1. How do you consider spam?
2. What are your actions in response to spam?
3. Would you be willing to pay an additional fee to your ISP if it provides the guarantee for a spam-free e-mail service?
4. Who do you think is the most appropriate to handle spam?

**D) About you**

1. Current location
2. Gender
3. Age group

In order to check if the prototype questionnaire could be clearly understood, it was administered on 17 October 2003 to twenty-three students of Middlesex University (Business Information Systems second-year undergraduate class). All the students said they understood the content of the questions. Useful feedback was derived.

- In QA3 ("Have you set up an e-mail account with this provider?"), if the answer is **no** then QB1 ("How many unsolicited e-mails do you get on average per day using your ISP's e-mail account?") is not valid. It would be possible at the end of QA3 to include the instruction "If your answer is **No** please do NOT reply to QB1". The instruction was not included, however, since it was too obvious.
- Students asked why in QC2 ("What are your actions in response to spam?") it was necessary to say "Tick one box only" instead of being allowed to tick more than one. According to the objectives of the survey the purpose of QC2 is to identify what is the most powerful action to tackle the problem of spam. A multiple choice would not be able to give such an answer.

Finally the questionnaire was given to Nick Paraskevopoulos (General Manager, NETFORCE Internet Business Services, Athens). NETFORCE is an internet marketing company and ISP that provides free web e-mail accounts to thousands of users. Mr Paraskevopoulos added several useful comments.

- In QC2 ("What are your actions in response to spam?"), an additional response could be to use the DNS blacklists. The response "Report spam to DNS Blacklists" was accordingly added.
- It might be interesting to include the question "What is the origin of spam you receive in your inbox?". It was judged, however, that this question would be more appropriate to ISPs than to users.
- Spam is not a type of communication, since there is no response from the recipient's side. Mr Paraskevopoulos preferred to talk about spam as cyber-pollution.

In February 2004, an opportunity arose to meet Professor Michel Walrave, Department of Communication Studies, Faculty of Political and Social Sciences, University of Antwerp, Belgium. During the meeting we reviewed the questionnaire and made a few further changes. He provided feedback based on the results of analysing 294 websites, published in his paper "Cyberkids' e-privacy at stake?" (Walrave, 2003). That paper summarised information concerning those who are responsible for data processing, its purpose and related privacy rights. Since 1992 Professor Walrave has conducted research on the implications of the information society, especially on data protection and direct marketing. Professor Walrave used as

a research instrument an online survey (of 93 items) among internet users and webmasters, to examine the quantity and quality of information in privacy statements. The main topics of his questionnaire were online processing of personal data, spam, types of data collected, cookies and e-mail privacy policies. This scanning of website forms was part of a programme of research concerning e-privacy and spam.

It was concluded from the discussion that, in order to identify the volume of spam per user, two further questions needed to be included: "how many e-mails do you get per day/week?" and "how many of those e-mails are spam?" It was decided to add another question to categorise users based on their online experience: inexperienced users tend not to understand the negative impact of spam and usually they have not purchased anti-spam software to tackle spam. Another added question was: "Was an anti-spam filter included in the ISP's/web-mail e-mail account or did you install it by yourself?"

- The ISP.
- I installed it.
- I don't have.
- I don't know.

The final version of the questionnaire, taking account of the above discussions, is included as Appendix A1.

## 4. Stakeholder analysis as a platform for an integrated approach

Stakeholder analysis was originally proposed (Freeman, 1984) as a tool for managers to engage proactively with their external environment in the face of a rapidly changing global marketplace. Additionally, Mitchell et al (1997) suggested a framework for stakeholder identification based on three criteria: power, legitimacy and urgency. Stakeholder analysis has been widely applied in strategic management, corporate governance (Burgoyne, 1994; Donaldson, 1995) as well as in information systems studies.

Stakeholder analysis has been used in this research. The major spam stakeholder groups were identified as well as their positions and potential roles in the UCE process. The views of authoritative stakeholders were elicited during several

workshops and conferences in Europe and the USA (a list is provided in Appendix D). A number of industry associations and individual companies, from ISPs and communications operators (mobile and fixed), through direct marketers and advertisers, to computer and software manufacturers, participated in the EU Workshop on Unsolicited Commercial Communication, held in the Charlemagne Building of the EU on 16 October 2003.

The framework of the stakeholder analysis was developed at the University of Illinois at Chicago and published at the 13th European Conference on Information Systems (ECIS 2005) which was held in Regensburg, Germany (see Appendix C6). Additionally the analysis was expanded and then published at the Internet Research Journal (see Appendix C1). The following table (Table 1), formed during the first stages of the stakeholder analysis, shows the major stakeholders of spam. ISPs represent the technical anti-spam solutions, government produces anti-spam legislation and organisations produce corporate e-mail policies.

***Table 1 – Stakeholder analysis for UCE***

| Stakeholder | Role | Actions to stop spam | Objectives |
|---|---|---|---|
| **Consumers** | Recipients of UCE | - Use of anti-spam technology<br>- Make e-mail addresses indistinct in html source code | - User awareness<br>- Should be aware that ISPs offer a choice of services |
| **Direct Marketing Associations** | Coordinate | - Develop codes of conduct and acceptable e-mail policies<br>- Ensure members comply with the DMA e-commerce code | DMA is committed to upholding its principles in order to combat spam while protecting legitimate e-mail marketing |
| **ISPs** | Develop, regulate, monitor | - Set up and maintain black/white lists on behalf of their subscribers<br>- Develop anti-spam solutions and Bayesian filtering | - Block UCE and minimise the occurrence of false positives<br>- Inform subscribers how to handle spam and cooperate with other stakeholders |
| **Government** | Legislate, enforce | - Produce legislation to secure the e-commerce environment<br>- Responsibility for implementation and enforcement<br>- Self-regulatory and technical issues<br>- Awareness issues | - Harmonise and enforce legislation across countries<br>- Cooperate with industry (filtering, codes of conduct)<br>- Consumer awareness |
| **Consumers' Privacy Associations** | Provide information Regulate Consult Educate | - Provide educational and awareness-raising programmes to empower consumers to make informed choices in relation to spam reduction strategies and technologies<br>- Operate reporting centres for complaints | Raise public awareness by informing consumers about spamming tactics and providing them with suggestions on how to block spam |
| **Organisations** | Receive Send | - Double role. Do not want to receive from third parties any UCE but most of them wish to use e-mail as a marketing tool | - Reduce the loss of productivity because of spam<br>- Remove their e-mail address from black lists. |

From that analysis, the next stages of the research were more clearly defined. The following sections describe the methods used to investigate legislation, technical anti-spam measures, and corporate e-mail policies.

## 5. Anti-spam legislation

One of the major stakeholders of spam is government: it produces anti-spam legislation in order to secure the e-commerce environment. Government is also responsible for implementation and enforcement issues, self-regulatory and technical issues, and awareness issues.

To determine the extent and possible impact of anti-spam legislation an evaluation and comparison of laws from selected OECD countries was carried out. Interviews with experts, and participation in conferences and workshops, yielded important secondary data on the current state of opinion on issues and potential solutions in the area of spam, and provided a rich picture of the status of current legislation in relation to spam.

**Methodology on legislative approaches**

**A) Evaluate and compare legal systems/frameworks**

Legal anti-spam systems/frameworks from Europe, USA, Canada, Australia, New Zealand and Japan were analysed and compared. All the above countries are members of the Organisation for Economic Co-operation and Development (OECD) and have identified that spam is a serious problem that needs to be tackled. At the beginning of the research, New Zealand had not enacted anti-spam legislation, the EU was debating between opt-in and opt-out scenarios, Japan was in favour of the opt-out approach, and in the USA the approach (opt-in v. opt-out) was varying among individual states. The evaluation and comparison of the different legal systems provided an understanding of how legislation has affected other stakeholders (i.e. spammers, ISPs, consumers, and marketing associations). It also showed that legislation can only partially address the problem of spam.

**B) Conduct interviews with experts**

Interviews with law experts provided valuable secondary data, especially because after the implementation of new directives there were not immediately any legal cases that could evaluate the effectiveness of new legislation. These interviews

also confirmed legislators as one of the major stakeholder classes in tackling the problem of spam. Anti-spam vendors have repeatedly expressed their uncertainty about whether legislation can entirely stop spam, and that was confirmed during the interviews.

Examples of the interviews and discussions (see also Appendix B) are as follows.

- Phil Jones, UK Data Protection Commissioner (Privacy and Spam): Wilmslow, 10 February 2004.
- Philippe Gerard, DG Information Society, European Commission: Brussels, 19 February 2004.

Interviews and a survey were also conducted with Atlantic Supermarkets SA in Athens, who use e-mail as a marketing tool, to examine how a legitimate e-business could easily make the mistake of infringing anti-spam legislation by sending unsolicited spam to users.

**C) Participate in conferences/workshops of governmental bodies**

Further information on current legislative approaches was gained from workshops and conferences, including the following.

- 4th ASEM Conference on e-Commerce, London (20–22 February 2005; http://www.asemec-london.org). Seminar themes: paperless trading, tackling spam, elogistics, elearning, ehealth.
- EU Workshop on Spam, Brussels (15 November 2004).
- EU Workshop on Unsolicited Commercial Communication or Spam, Brussels (16 October 2003). A number of issues were discussed at the workshop in relation to the new rules (opt-in), and practical information was given on acceptable marketing practices under the opt-in regime including clarification of legitimate collection of personal data. In addition, practical information was provided on how to avoid UCE and on steps that individuals and organisations could take when confronted with spam, including complaints mechanisms and possible alternative dispute resolutions systems. The workshop was useful since the views of various authoritative stakeholders were provided. Various EU authorities confirmed the outcomes from earlier interviews with legal experts. More specifically, one of the outcomes of the interview with Philippe Gerard confirmed what had been said at the EU Workshop on spam: though

EU anti-spam legislation had been recently implemented, the harmonisation of national legislation among the member states appeared to be a difficult procedure.

**D) List European and American legal cases**

The list included spam legal cases. In order to select the statutes on IT and e-commerce, on-line resources such as Lexis and Lawtel were used. This led to a better understanding of the legislation related to spam. The following are examples of legal cases in relation to spam.

- UK-based BiblioTech rejected attempts by US spammers to settle a suit filed in the USA. A settlement offer had been put to it which included compensation, but one US company refused to be bound not to repeat the spamming and BiblioTech wanted those it sued to undertake not to engage in this activity again.
- Virgin issued a writ against Adrian Paris, a Surrey businessman, for damages for breach of contract and trespass, after he allegedly sent out 250.000 junk e-mails on behalf of Pro-Photo UK using a Virgin Net account. The case settled.

A research paper, "Combating spam through legislation: a comparative analysis of US and European approaches" (see Appendix C4), was submitted and accepted at the 2nd Conference on E-mail and Anti-Spam (CEAS 2005) 21–22 July 21 2005 at Stanford University, Palo Alto (in cooperation with the International Association for Cryptologic Research and the IEEE Technical Committee on Security and Privacy).

## 6. Technical aspects

Another approach that can be used to resolve the problem of spam is technology. The stakeholder analysis (Table 1, above) showed that anti-spam software or hardware solutions are usually developed by ISPs or anti-spam vendors. They include the setting up and maintenance of black/white lists for the benefit of their subscribers, the development of 1st- and 2nd-generation technical solutions and Bayesian filtering. However, despite the implementation of anti-spam technologies, the problem of spam is not resolved. This aspect of the research sets out to identify the different technical approaches to combat spam, and to assess their effectiveness.

## Methodology for the anti-spam technical measures

### A) Create a template for evaluation

Technical anti-spam solutions were classified as follows.

- 1st-generation anti-spam measures.
- 2nd-generation anti-spam measures.
- Client solutions.
- Outsourced anti-spam measures.

The evaluation template, based on signal detection theory, compared whether a technical measure identifies a message as spam with whether it actually is spam (Heeger, 2003): see Table 2.

***Table 2 – Signal detection theory (statistical decision)***

| | | **What actually happens** | |
|---|---|---|---|
| | | **No** | **Yes** |
| **Response** | **Yes** | **F+**<br>False positive | **Hit**<br>Correct hit |
| | **No** | **True**<br>Legitimate e-mail | **Miss**<br>Spam that is not tagged as spam |

"Response" is the outcome of an anti-spam software filter saying whether an e-mail message is spam or not. "What actually happens" means whether an e-mail message is actually spam or not. When the anti-spam software filter misidentifies a legitimate e-mail message as spam then that is considered as a false positive (F+). When spam has not been tagged as spam by the filter, that is a Miss. The other two cases reflect when the anti-spam software filter categorises successfully an e-mail either as spam (Hit) or as legitimate (True). Evaluation using this template revealed the degree of successful identification by a filter.

### B) Select secondary resources

- Participation in IT conferences/exhibitions: further information on current anti-spam technical approaches was gained from workshops and conferences such as the following.

- EEMA conference "Spam the death of e-mail?" Dublin (3–4 December 2003; http://www.eema.org/spamconference/programme.asp). Stakeholders such as the Irish Parliament, Microsoft Corporation, the European Commission, the Direct Marketing Association and Royal Mail presented papers on spam, addressed areas of legislation, and discussed the impact on e-commerce and the consequences of the EU harmonisation proposals. Finally, the question of what kind of technology needs to be in place, and whether it will be in place in time to support the new anti-spam legislation, was discussed.
- Conference/exhibition "Computer and Internet Crime 2004", London (March 2004; http://www.cic-exhibition.com).
- Infosecurity conference "Europe 2004", London (April 2004).

- Interviews with IT experts: a number of IT professionals in the UK, Greece and the USA were interviewed in the area of e-mail security. A sample of questions that were addressed during the interviews follows.
  - What is the role of the ISP when we try to combat spam?
  - Who should be in charge for the categorisation of spam?
  - What kind of relationship should an ISP develop with other spam stakeholders?

  The IT experts concluded that individuals should be in charge for the categorisation of spam. That could be a decision made at any time before the user receives e-mail or during the subscription process with an ISP. ISPs in cooperation with marketing associations may create selective commercial databases with legitimate registered companies. These companies can send legitimate commercial communication to the users of ISPs.

After the technical issues were investigated in depth, a research paper was submitted and presented at ETHICOMP 2004 "Challenges for the Citizen of the Information Society" (see Appendix C7).

## 7. Organisations – corporate e-mail policy

From the initial stakeholder analysis (Table 1 above), the role of organisations in the spam context is to combat lost productivity. Part of this research was to develop a

corporate e-mail policy and to evaluate its impact on incoming spam. Atlantic Supermarkets SA were consulted, and agreed to test the e-mail policy. In terms of turnover, Atlantic is the tenth largest commercial enterprise in Greece and the fifth largest in its sector. It serves more than 2,500,000 customers per month and employs more than 4,500 people. The level of spam was significantly large (75% of incoming mail was spam), and it created a major problem for the company's development of e-commerce. Spam constituted a great cost for the organisation, consuming precious network resources and employee time. It also carried serious legal liability as well as network security risks. There were also reported instances of hidden e-mail threats such as viruses that were attached in spam e-mail messages. This part of the research will be discussed in the chapter on corporate e-mail policy.

**Methodology for corporate e-mail policy**

A) **Select and evaluate policies**

AOL, Yahoo!, MSN, Google, ICQ, EU, NHS and Barclays Plc were selected as organisations whose policies should be studied and evaluated.

B) **Conduct interviews**

Interviews were conducted with IT managers and law experts in the area of corporate e-mail policy. To meet the need for spam-related e-mail policy and to determine the cost of spam and the value of anti-spam solutions, over twenty managers were interviewed. The interviews were used in part to select material about what should be included in e-mail policies. The interviews led to conclusions such as the following.

- E-mail policy is an essential element for the corporation.
- Many companies do not have clear e-mail policies.
- Employees need education and training to improve their behaviour towards spam.

C) **Conduct corporate survey**

A survey questionnaire was administered at Atlantic Supermarkets SA ("How employees react to spam": see Appendix A2). It provided data on employees' experience of spam, how they react to it, and whether they consider it a problem.

D) **Develop experimental corporate e-mail policy**

The survey at Atlantic was followed by designing an e-mail policy for the company, which was approved and implemented by the IT Department. This constituted a piece of action research within the overall research design. The question was whether the implementation of the corporate e-mail policy would result in a decrease in the level of spam because it provided clear guidelines to employees on how to handle spam and in general how to use e-mail appropriately within the organisation. This question and the subject of corporate e-mail policy are discussed in Chapter 8.

The topic of tackling spam with the assistance of a corporate e-mail policy was investigated in depth and at the end a research paper was submitted and published at the International Conference on Information Warfare and Security (ICIW 2006) at the University of Maryland Eastern Shore, USA (see Appendix C2).

## 8. Academic visit to the USA – University of Illinois at Chicago

Toward the end of the research period an opportunity arose to visit the USA by invitation/scholarship of the University of Illinois at Chicago (UIC). The visit furthered the research since it was possible to investigate the culture of sending spam in the USA (the vast majority of spam originates in the USA), to review anti-spam technologies (the latest anti-spam technologies have been developed in the USA) and to explore legislation further: it transpired that the US anti-spam legislation adopted an opt-out system different from the opt-in approaches in the EU, Canada, Australia (opt-in).

The visit to the States gave the opportunity to compare the perception of the problem, and the various approaches to dealing with it, in the UK and the USA. The research in the USA was based on the research approach used in the UK prior to the visit in order to maintain consistency.

- **Participation in conferences/workshops in the USA**

  Further information on current anti-spam technical and legal approaches was gained from workshops and conferences such as the 14th Virus Bulletin International Conference and the E-mail Marketing Conference, held in Chicago in 2004.

- **Selection of secondary resources**
  - Legal issues
    - Conduct interviews with legal experts.
    - Select secondary resources. Compare different surveys about spam legislation.
    - Create a database with American legal cases in relation to spam.
  - Technical issues
    - Template and evaluate different types of anti-spamming packages.
    - Select secondary resources. Compare different surveys for technical anti-spam issues.
  - Corporate users
    - Conduct open public survey (questionnaire) "How users react to spam".
    - Select and evaluate different online policies related to spam.

## 9. Summary

This chapter has described the various research methods used to address the different areas (legal, technical and organisational). The stakeholder analysis provided the categories for investigation. It provided methods for discovering the extent of the spam problem, investigating the international anti-spam regulatory framework, evaluating technical anti-spam solutions and developing corporate e-mail policies.

# CHAPTER 4 UNSOLICITED COMMERCIAL E-MAIL: SPAM

## 1. Introduction

As explained in chapter 3 (on methodology), one of the first steps of the research was to identify the scope of the problem and how individuals and organisations react to spam. This aspect was approached initially by conducting an open survey with the use of a questionnaire, and later on by conducting interviews with IT specialists in the area of spam from ISPs and anti-spam software companies. This chapter defines the term of unsolicited commercial e-mail and describes the different types of spam and the kinds of spam with which internet users are confronted. Based on the definitions and characteristics of UCE, a typology of spam is later developed. The chapter also examines different methods and various strategies of sending spam, such as harvesting, spam-botting and dictionary attacks, and shows that there is a direct relationship between spam and cyber crime in the form of 'phishing'.

## 2. What is unsolicited commercial communication?

The term 'spam' was used in the Monty Python skit (Monty Python sketch, 1970) in which the spam meat product was featured. In this skit, a group of Vikings sang a chorus of 'spam, spam, spam...' in an increasing crescendo in a restaurant where everything on menu included spam. Spam is commonly used to describe unsolicited, often bulk e-mails (Langford, 2000). According to Turban et al. (2000) spam or UCE is defined as "the practice of indiscriminate distribution of messages without permission of the receiver and without consideration for the messages' appropriateness". The above definitions consider the permission from receivers, and the quantity of mails sent, to describe UCE. The Direct Marketing Association's definition reflects both these characteristics: "The act of sending unsolicited bulk commercial e-mails to an individual's e-mail address without having an existing or prior business/personal relationship or obtaining consent/permission" (Direct Marketing Association, 2003).

Those definitions of spam take a recipient perspective, without taking into consideration the sender. However, UCE includes the term "commercial", reflecting the goal of the sender – it implies a commercial intent such as advertising, marketing

or promotion. In 2002, the Australian National Office for the Information Economy (NOIE), while conducting an extensive review of spam, encountered the difficulty of trying to define the term. In its review NOIE, while recommending further work on a widely recognised and accepted definition, did develop a working definition: it defined spam e-mail as a communication that could not be reasonably assumed to be wanted or expected by a recipient. The above definition is adopted in the current research. The primary concern of this thesis is with unsolicited communications that have a commercial intent. UCE is different from other unsolicited e-mails such as chain letters containing jokes, religious promotion material, etc. However the growth of UCE and its variants have resulted in non-commercial, malicious outcomes as well. Several UCE messages serve as carriers and distributors of viruses that could potentially be harmful to the recipient.

Given the evolution of spam and its changed characteristics, spam could be categorised into multiple types.

***Table 3 – Types of spam: Federal Trade Commission***

| | |
|---|---|
| **Junk e-mail** | Bulk sending of unwanted commercial e-mailing |
| **Non-commercial spam** | Bulk sending of unsolicited e-mailing without commercial interest, such as chain letters |
| **Offensive spam** | Bulk sending of mailings with adult-oriented content (e.g. pornography) |
| **Spam scams** | Bulk sending of fraudulent mailings with the intention to invade the privacy of the recipient |
| **Malicious** | Mass mailings that contain malicious program code such as viruses and Trojans. |

Based on the content of spam, the Federal Trade Commission (Federal Trade Commission, 2003) classified UCE into the several categories (Table 4). The issue of UCE spans a number of internet user groups ranging from online users to internet service providers and policy-makers.

***Table 4 –Types of UCE: Federal Trade Commission***

| Content | Description |
|---|---|
| **Business opportunities** | Work-at-home, franchise, chain letters |
| **Adult** | Pornography, dating services, etc |
| **Finance** | Credit cards, refinancing, insurance, foreign money offers etc |
| **Products/Services** | Products and services, other than those coded with greater specificity |
| **Health** | Dietary supplements, disease prevention, organ enlargement, beauty products |
| **Computers/Internet** | Web hosting, domain name registration, e-mail marketing |
| **Leisure/Travel** | Vacation opportunities |
| **Education** | Diplomas, job training |
| **Other** | Types of offers not captured by specific categories listed above |

## 3. The negative impact of UCE

UCE has reached a point where it creates a major problem for the development of e-commerce and the information society. MessageLabs, a respected source of data and analysis for e-mail security issues, trends and statistics, which gained world-wide recognition as the first company to stop and name the 'LoveBug' virus in May 2000, say that about 30% of all e-mail sent in November 2003 was spam and that the rate is increasing rapidly. Moreover, in 2003 there was an increase in malicious spam, such as financial scams (Wood, 2003).

The EU member states, industry and consumers all have a role to play in the fight against spam both at national and international levels (EU Brussels Workshop, 2003). This workshop was aimed at discussing additional measures needed to address the various legal, technical and educational aspects of spam: effective enforcement by public authorities, cooperation within industry (filtering, codes of conduct), consumer awareness, and international cooperation. The suppliers of technical solutions noted the continuous game of catch-up that is being played out, summarised by Gert Veendal: "It is a battle between anti-spam programmers and spam marketers". As soon as a new anti-spam software package is released in the market, spammers are looking for a new way around it. (Veendal, 2003).

While e-mail may be a boon for advertisers, it is a problem for consumers, corporations and ISPs. Spam also impinges on the privacy (Meade, 2003) of individual internet users. It can also cost users in terms of the time spent reading and deleting the messages, as well as in a traditional economic sense where users pay time-based connection fees. Junk e-mail not only costs corporations dearly in precious network resources and employee productivity but also carries with it serious legal liability as well as network security risks. Spam fills corporate mailboxes making it difficult for users to find important messages (Kille, 2003). It has also been reported (Gradwell, 2003) that instances of hidden e-mail threats such as viruses (MailWasher, 2001b) that are included in spam e-mail messages are on the increase. Spam, which most frequently takes the form of mass mailing advertisements, is a violation of internet etiquette (EEMA 2002). The open survey (see Chapter 3 on methodology) confirmed the positions of anti-spam vendors and European Union regarding the negative impact of spam by concluding that the vast majority of internet users (97%) considered spam as a serious problem that can be harmful.

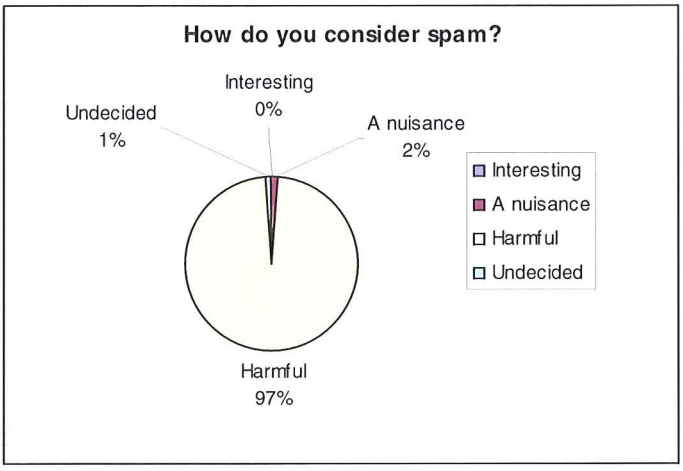



*Figure 2 – How do you consider spam?*

Moreover, based on the results of the open survey, the answer about which stakeholder is most capable to tackle spam varied: ISPs 28%, government 30%, marketing associations 18%, on-line users 22%, other 2%.

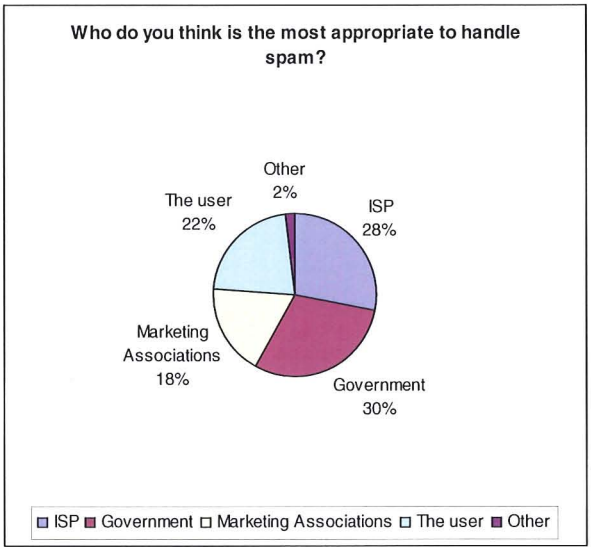



*Figure 3 – Who do you think is most appropriate to handle spam?*

Figure 3 suggests that people believe that different groups may be responsible for addressing the problem. This led to the next stage of the research, which was to use stakeholder analysis as an approach to investigate further the problem. The questionnaires also showed that spam is a serious problem, confronting the majority of users. 36% replied that they receive on average 6–10 spam e-mail messages per day, while 40% receive 11–16.

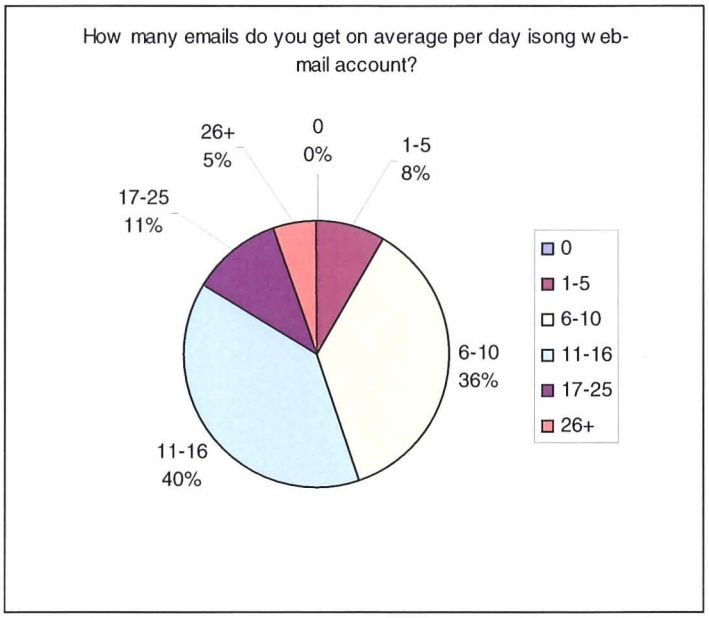



*Figure 4 – How many e-mails do you get on average per day using web-mail account?*

The following table is an initial attempt to categorise the negative effects of spam to various groups.

*Table 5 – Problems associated with spam*

| Cyber community | Problems associated with spam |
|---|---|
| **Individuals** | - Spam impinges on the privacy of individual internet users<br>- 'E-mail harvesting' collects bulk e-mail addresses<br>- E-mails usually contain malicious program code that harms the computer or network<br>- Stealing of critical customer information such as credit card information<br>- Phishing scams (forged identities) |
| **Employees and corporations** | - Time spent reading and deleting messages<br>- Additional cost for time-based connection fees<br>- Lost productivity |
| **ISPs** | - Cost of providing anti-spam infrastructure<br>- Cost of extra bandwidth and storage to cope with the volume of spam<br>- Operating systems have collapsed due to the volume of spam<br>- Customer dissatisfaction |
| **E-commerce environment** | - Decrease of consumer confidence and trust<br>- Extravagant earnings<br>- Quack products undermine credibility of genuine ones<br>- Illegally pirated software and other digital products |
| **Governmental agencies** | - Violation of internet etiquette<br>- Spam can be offensive / pornographic material – violating laws |

## 4. A typology of spam

This section identifies two distinct characteristics of UCE. First is the origin of UCE, whether the e-mail was an outcome of an intended or unintended action of the recipient. Intended actions include voluntarily providing e-mail address to some web sites or online stores, or performing some online or offline transaction. Here, the user has explicit knowledge that the e-mail address is being given out, as he/she initiated such an action. On the other hand, it is also possible that the e-mail address could also have been compiled by a third party without the explicit knowledge or consent of the recipient. Second is the extent of negative impacts of UCE, which could vary from being useful to a recipient, through causing minor disturbance, to causing major negative outcomes such as a virus attack.

Based on those two dimensions, a typology of UCE is proposed that delineates four types (Table 6). This approach is consistent with Khong (2004) who categorised spam into e-mails that relate to 'contract offer' and those that are 'nuisance'.

These four types are described in the next table.

***Table 6 – Proposed typology of UCE***

| | | | |
|---|---|---|---|
| **Recipient's consent** | Without consent | | III, IV |
| | With consent | I, II | |
| | | Low | High |
| | | **Potential negative impact** | |

***Type I.*** This type of UCE represents a direct relationship between the sender and recipient. The relationship assumes some degree of legitimacy, as the recipient provides explicit consent to receive direct e-mail marketing. This consent could be given through web forms, e-mail requests or through other explicit means of subscription (opt-in methods). Typically, there is a provision to opt-out of the relationship, as the recipient could request termination of communication at any point in time. An important characteristic of type I UCE is that the identity and contact details of the sender are known to the recipient. In the USA, a sender could send UCE without the explicit consent of the receiver, and this action would be considered

legitimate provided the sender fulfils some basic requirements such as revealing his identity and contact details, and provides a way for recipients to opt out of the communication. Some states in the USA mandate marketers to use the term "ADV" in the subject line of the messages to declare explicitly that the mail is marketing-related.

***Type II.*** This type of communication can be described as an indirect, permission-based partnership. When consumers complete some kind of on-line transaction, they are asked to opt in to certain e-mail lists of related services or affiliates. Information about consumers is sent to affiliates and other third parties, who may initiate communication with the recipients. The consumers may not be aware of these third parties at the time of providing their permission. Several direct marketing associations also maintain mailing lists of consumers who have provided them with their contact information. Typically, the consumers could request termination of communication as well.

***Type III.*** This category includes spam that originates from third parties without explicit permission or consent of recipients. E-mail databases compiled from public domains and free e-mail services, and web-sites with non-secure transmission of personal information through on-line forms, typically serve as primary sources of consumer contact information. Sometimes, spammers employ search bots that navigate the internet and automatically retrieve e-mail addresses from public areas. Sometimes, they also forge the headers of their e-mail in an attempt to avoid losing their accounts and to evade e-mail filters. Much offensive spam falls in this category. The opt-out links at the bottom of spam mail may not work, but are often used to verify the validity of the recipient's e-mail address.

***Type IV.*** In this category, the identity of senders is unknown and the intention of the spammers extends beyond simple commercial purposes to being potentially harmful to the recipients. Spammers could implant viruses, spy code, malicious software, or other potentially damaging tools in the e-mail that could harm the recipient. Sometimes, the malicious code could stay inside the recipient's computer, intruding into privacy, retrieving information about the recipient and sending it back. In many cases, consumers may not even be aware of the presence of malicious code, and have little knowledge of it.

# 5. Spammers' techniques to select e-mail addresses and ways to tackle the problem

Spammers use various techniques to locate e-mail addresses on the internet. "E-mail harvesting" is the method of surreptitiously collecting bulk e-mail addresses from public or private sources. Spammers employ search bots that navigate the internet and automatically retrieve e-mail addresses from public areas such as web pages, chat rooms, e-mail lists, newsgroups and online directories. These e-mail addresses are then collected for use by the spammer. Every web page has a source code which instructs the web browser how to display the content. Search bots scan the source code of web pages for normal text e-mail addresses (e.g. e.moustakas@mdx.ac.uk). 'Sam Spade' is a tool that can search websites for e-mail addresses. In order for spammers to identify whether or not an e-mail address is valid they use scripts to open a connection to the target mail server, submit millions of random e-mail addresses and then use the 'VRFY' command to verify if addresses are live. Another method known as 'dictionary attack' was used several times against Hotmail web-mail accounts. Search engines such as Google could also be a great resource for spammers to collect e-mail addresses to send UCE. Spammers could type on the search tab the character '@' and they will retrieve a list of findings that include e-mail addresses. Spam can bypass content filtering tools by using "hash busting" techniques like hyphens to break known search terms. For example a computer will not identify the words *V-i-a-g-r-a* and *viagra* as the same – though a human being will.

There are a number of steps that can be taken to prevent an e-mail address from being scanned by search bots. First, e-mail addresses should not be allowed to be given by employees to third parties across public forums such as chat rooms or newsgroups. An appropriate e-mail policy is essential to regulate this in the workplace (discussed later in Chapter 8). Second, the company should decide if the corporate e-mail address will be displayed on the web-site. A number of techniques that could be used to prevent spammers from capturing e-mail addresses are discussed in the following paragraphs.

## 5.1 The 'munging' technique

Individuals can add additional letters (e.moustakas@mdx.REMOVE-THIS.ac.uk) or spaces (e.moustakas @ mdx ac uk) to e-mail addresses in order to confuse search bots. That is called "munging". On-line readers may remove the word 'REMOVE-

THIS' in the e-mail address or ignore the spaces. However this technique is not 100% effective since several spamming programs automatically remove words such as 'REMOVE-THIS' and 'NO-SPAM' from e-mail addresses or remove spaces where they are present. Also the above technique is not effective where a spammer employs another individual to search for e-mail addresses. Finally, this technique might be confusing for users who might not remove the extra letters or spaces.

### 5.2 Make e-mail addresses indistinct in the .html source code

It is recommended that an e-mail address should not be displayed in normal plain text in the source code of a web page in order not to be captured easily by a search bot. The characters can be replaced either by a small image where the e-mail address will be displayed, or replaced with the use of "hexadecimal encoding". In hexadecimal encoding the e-mail address e.moustakas@mdx.ac.uk is transformed as follows in the source code:

*<a href="mailto:%6b%61%73%40%6d%64%78%2e%61%63%2e%75%6b">contact</a>.*

There are web pages on-line that can transform regular e-mail addresses to hexadecimal format for free, such as http://www.wbwip.com/wbw/e-mailencoder.html.

### 5.3 On-line contact forms

Maybe the only foolproof technique to prevent search bots from finding e-mail addresses is by not displaying e-mail addresses at all on a web site. To ensure that internet users can still contact an organisation by means of e-mail the web developer needs to create an online "contact form". The web page may include the names and the positions of staff, so that if a reader wishes to contact a member of staff (s)he needs to click on the name or on a link provided for that purpose. When the internet user clicks on the link, an on-line contact form is displayed, where a message can be composed. Therefore, the e-mail address is never displayed to the internet user or on the web page.

## 6. Spam and cyber fraud

At the beginning of this chapter a new type of cyber fraud, originated through spam, was noted: it is known as "phishing". This is a form of electronic identity theft which

is not only financially and personally damaging, threatening to consumer confidence and undermining e-commerce, but which also carries a more serious threat. Phishing assists cyber-crime (Dearsley, 2004) and, according to the National High-Tech Crime Unit (UK), is usually perpetrated by organised crime groups often based in Eastern Europe and the former Soviet Union (NHTCU 2004).

Taking measures to reduce the growth of on-line identity theft has become a top priority for any organisation that wishes to leverage the internet to extend services to customers and trusted third parties. The next section discusses the growth of on-line fraud as a result of phishing techniques. An explanation of phishing and its relationship with spam follows, exposing some of the tricks used by phishers. The second part of the chapter assesses the various approaches needed to overcome the problems posed by this threat, by analysing the various roles of the participants and the technology. Finally, recommendations are given to combat this type of cyber fraud as well as suggestions for consumer defence through technology and education.

## 7. Growth and negative impact of on-line fraud

The theft of identity and financial information is a growing problem in terms of magnitude and awareness. The target could be any organisation with financial information on-line (Symantec, 2004). Financial identity theft occurs when personal information is used by a third party without the knowledge or consent of the owner. The UK government estimates that more than one hundred thousand people are affected by identity theft in the UK each year, costing the British economy over £1.3 billion annually (Cabinet Office, 2002). Figures show that 4% of the UK's on-line account holders automatically respond to e-mails that appear to come from their bank. In addition, technical security measures are not used – roughly 25% have no updated virus checker on their computers, while more than 40% do not have an active firewall (Identity Theft Resource Centre, 2004). The UK is not the only country that is targeted. The USA, Australia, New Zealand and Canada are also included in the scams. According to the United States Federal Trade Commission, identity theft is America's fastest growing crime, with losses estimated to be billions of dollars each year (Federal Trade Commission, 2003). The following section gives the background and context of phishing.

## 8. Explaining phishing

The term phishing comes from the analogy that scammers are using e-mail to fish for personal information such as passwords and credit card details from the sea of internet users. It has its origins in the 1960s term "phone phreaks" (Anderson, 2001). The adoption of the "ph" in place of "f" by hackers in the early years of hacking into the telephone system has been continued in the term phishing. In the 1960s and '70s, phreaking usually involved building devices that could trick telephone systems into believing that the phreaker's instructions were originating from the telephone company's internal systems (Finley, 2000).

According to the Anti-Phishing Working Group (APWG), an industry association focused on eliminating identity theft and fraud resulting from the growing problem of phishing, one of the first recorded phishing cases was in 1996 – hackers were stealing AOL's e-mail accounts by scamming passwords of unsuspected AOL users.

Phishing is a form of online identity theft that uses spoofed e-mails (when a user receives an e-mail that appears to have originated from one source when it actually was sent from another source) designed to lure recipients to fraudulent websites in order to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. (Anti-Phishing Working Group, 2004).

The rapid increase of phishing attacks may be no more than a reflection of the general explosion in spam messages, and taken as part of the whole spam problem. However, the impact of phishing has a more threatening dimension. Spam traditionally has been seen, at best, as a nuisance in using e-mail resources and taking user time (and in the case where users are employees, company time), and at worst the carrier of dubious content, or viruses. Companies and users were the passive recipients of random e-mail marketing – in other words they were arbitrary victims who shared roughly equal costs (resources, damage to data, personal time). Victims of phishing attacks, though, experience a different type of loss. Users lose control of their personal data, and companies suffer financial loss as well as loss of confidence by customers in using on-line facilities. These losses pose a fundamental threat to e-commerce. In phishing attacks, the level of damage, the focus of attack, and the groups targeted, are different from the ones of general spam (University of Houston, 2005), and the consequences

move beyond costs to individuals and companies in time and technical solutions to a situation that threatens the whole concept of e-commerce (Schneider, 2004). The following table (Table 7) summarises the major differences between spam and phishing as analysed above.

*Table 7 – The major differences between spam and phishing*

| Context | Spam | Phishing |
|---|---|---|
| **E-mail** | Often authentic, promoting a real product or service | Phishing e-mail messages are based on fraud and deceit |
| **Range of damage for businesses** | Internal | External |
| **Organisational assets attacked** | IT resources | Brand |
| **Key threat** | Ability to use e-mail as a communication tool | Ability to do business online |
| **Group targeted** | Employees | Customers and potential customers |
| **Attention-seeking** | Often seek attention | Avoid attention |

# 9. Methods used by phishers

The people behind this scam use multiple methods to commit phishing attacks, including deceptive subject lines, forging e-mail headers and disguising the links within e-mails. Messages often appear to be legitimate, and only after investigating URLs do they turn out to be fraudulent.

## 9.1 Collecting information using html forms

E-mail messages either can be composed in plain text or can be formatted as mini web pages, capable of displaying graphics or formatted text or even of running scripts. That makes phishing a much easier task. The following figure presents the case where an html-based form is integrated within an html-formatted e-mail, the code in the form is hidden and as a result the phisher is able to hide a bogus URL in a *submit* button that the user presses after entering his personal information.


*Figure 5 – Phishing case I: html forms*

## 9.2 Trojan horses and malicious JavaScript

A Trojan horse is malicious program code that can be installed in a computer by a user who thinks that the file is software, a game, a system utility or even a browser plug-in. It can act as a spy camera that can capture passwords or account numbers, or it can install programs to take screenshots of the system which are then forwarded to the phisher. According to the Anti-Phishing Working Group one of the most sophisticated phishing techniques involves the use of JavaScript programming language to create a fake browser address bar in the browser. When the user types in an address, the malicious code will direct them to the fraudster's web site.

## 9.3 Imitation of reputable companies' web sites

A successful phishing e-mail will mimic genuine logos and text from original web sites. The most common way to mimic a reputable company is to adopt the company's visible branding and corporate identity. In the e-mail shown below, the fraudsters pulled the Paypal logo from the Paypal site.

PayPal

Dear cohhelp@email.arizona.edu,

It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information.
Failure to update your records will result in account termination. Please update your records in maximum 24 hours. Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.
Please click here to update your billing records.

*Figure 6 – Phishing case II: Paypal logo*

Additionally phishing e-mail messages may use the TRUSTe symbol at the bottom of an e-mail (see the example reproduced below).

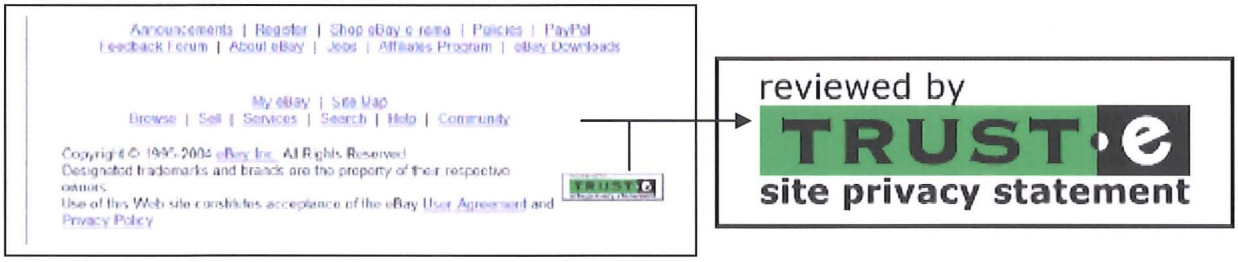



*Figure 7 – Phishing case III: TRUSTe symbol*

The TRUSTe symbol is designed for use by businesses that have a high standard of personal information protection.

## 9.4 Fake reply e-mail address

In phishing e-mails, the e-mail claims to be from a reputable company, but is set to reply to a fraudulent reply address. In the example below, this fraudulent ebEy e-mail claims to be from ebay support, but is set to reply to confirm@ebey.com.

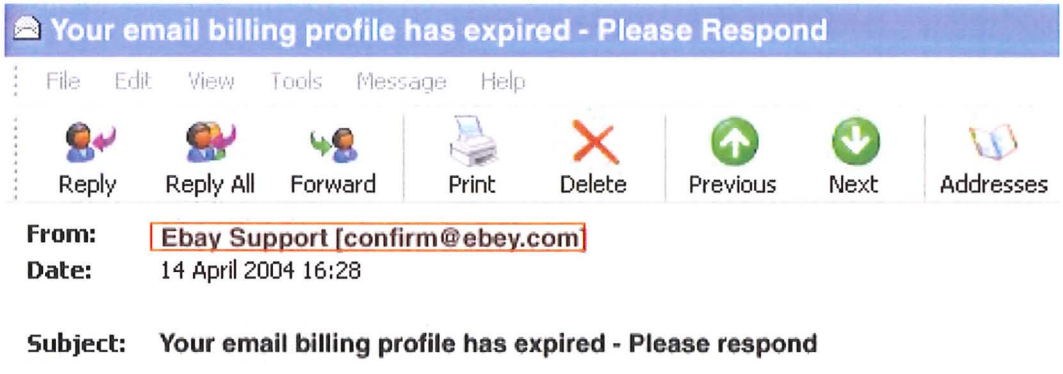



*Figure 8 – Phishing case IV: Fraudulent reply addresses*

## 9.5 Fake secure connection

When a URL begins with https:// instead of http://, it indicates that information is transmitted through a secure connection – server (SSL certificate). However some fraudulent web sites use an https:// URL to appear as a genuine site. The following example is a fraudulent PayPal web-site that used this technique.

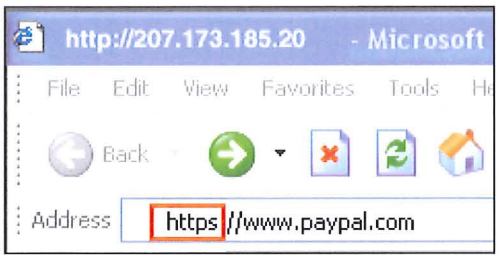
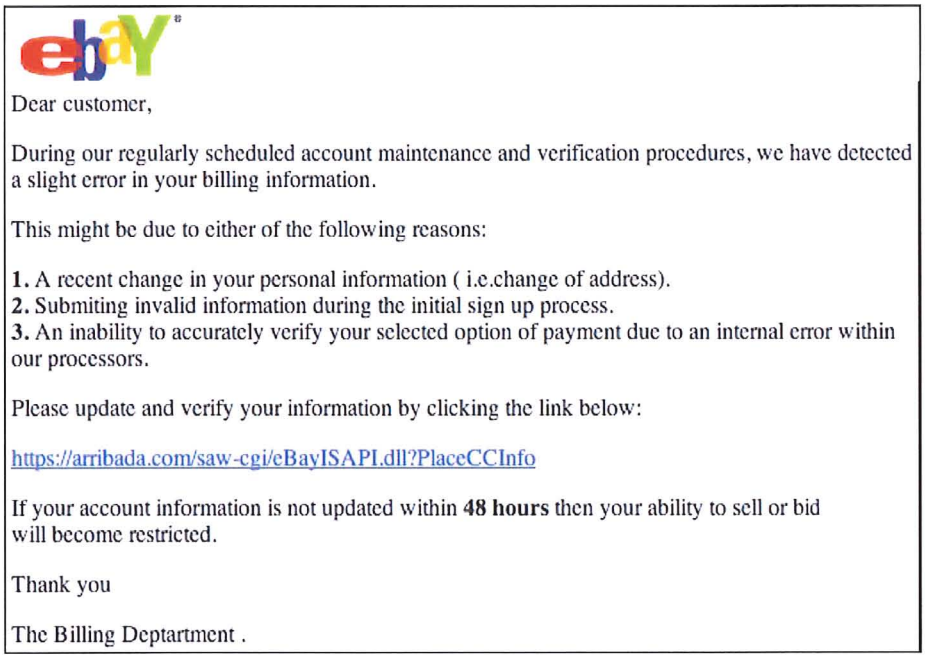



*Figure 9 – Phishing case V: Fraudulent web site using https://*

## 9.6 How to catch the phish fast

After convincing the consumer that the e-mail message originates from a reputable company, the next step is to obtain sensitive information. In hopes of gaining the consumer's trust, phishing e-mails also try to assure the individual that the transaction is secure and that personal information will be kept confidential. Therefore the fraud message might be stating that the company needs to update the user's records, or that the recipient's account information is outdated, or that a credit card has expired. In the e-mail shown below, the fraudsters inform the ebay consumer that (s)he has to re-enter personal information within the next 48 hours.



Dear customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

**1.** A recent change in your personal information ( i.e.change of address).
**2.** Submiting invalid information during the initial sign up process.
**3.** An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below:

https://arribada.com/saw-cgi/eBayISAPI.dll?PlaceCCInfo

If your account information is not updated within **48 hours** then your ability to sell or bid will become restricted.

Thank you

The Billing Deptartment .

*Figure 10 – Phishing case VI: ebay*

## 9.7 Link to web sites that gather information

Most phishing e-mails provide a link that takes the recipient to a fraudulent web site instead of using forms within the e-mail. For example the HTML code <A href="http://www.fakecompany.com">http://www.legitimatecompany.com</A> displays http://www.legitimatecompany.com though it takes the user to a fake web site when clicked. Furthermore the address bar can be turned off and replaced with a fake one that can fool the users. When the victim clicks on the link, the internet browser will open a web site with a URL that may be very similar to the one they would expect. Phishers usually register domain names with similar looking addresses or using character replacement (using the number "1" for the lowercase letter "L"). Many people could be fooled since they may not notice the difference in the address. In the e-mail shown below, the fraudsters ask Citibank customers to update their personal information to avoid termination of their account.

citi

Dear Citibank valued member

Due to concerns, for the safety and integrity of the online
banking community we have issued this warning message.

It has come to our attention that your account information needs
to be updated due to inactive members, frauds and spoof reports.
If you could please take 5-10 minutes out of your online experience and renew
your records you will not run into any future problems with the online service.
However, failure to update your records will result in account suspension
This notification expires on **Aug 10, 2004**.

Once you have updated your account records your internet banking
service will not be interrupted and will continue as normal.

Please follow the link below
and renew your account information:

https://www.citibank.com/update/update.htm

Sincerely,
**Citibank customer department**

***Figure 11 – Phishing case VII: Citibank***

## 9.8 The loopholes of the DNS

There are several security issues with the Domain Naming System (DNS), which is a hierarchical database that is responsible for converting the numerical Internet Protocol (IP) numbers to readable names. On-line fraudsters take advantage of these security loopholes to hijack a domain and redirect traffic from a genuine to a malicious web site. In other cases fraudsters can register a new domain name that is very similar to a legitimate domain. Two recent incidents that involved a phishing scam involved the domains www.ebay.com and www.msn.com. The fraudulent domain names www.ebEy.com and www.billing-msn.org were not associated with ebay or MSN, but they appeared convincing to unsuspecting users. In the e-mail shown below, the fraudsters ask MSN members to update their account information to prevent access being blocked.

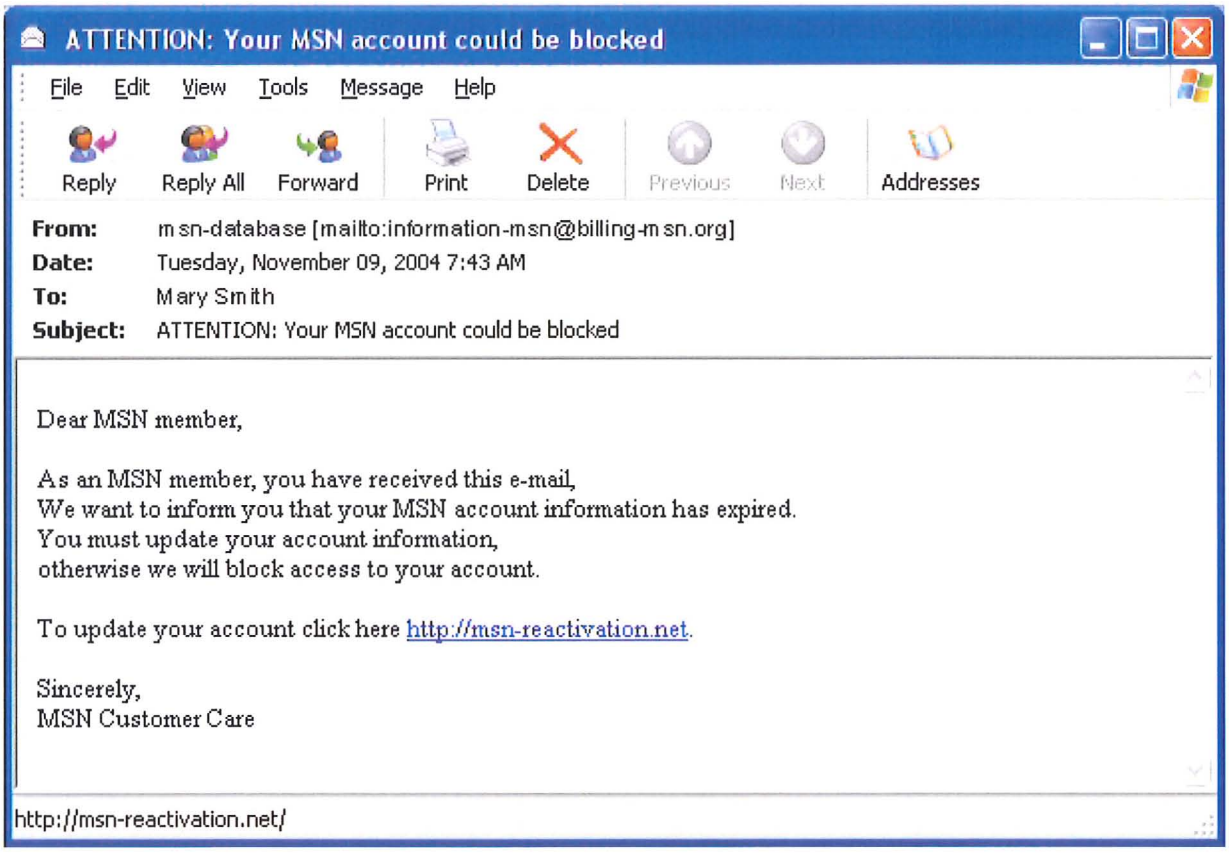



*Figure 12 – Phishing case VIII: MSN*

## 9.9 Social engineering

The term social engineering was initially used in political science as an attempt by government or private groups to engineer (i.e. change) the views and behaviour of citizens. In computer security, social engineering means the practice of making an

individual believe that they are dealing with a legitimate person or a genuine company when in fact they are not (US Department of Homeland Security, 2004). Fake e-mails used in phishing schemes claim to be from trusted parties, so that users are more likely to trust their contents.

## 10. Mechanisms for tackling phishing

This section begins with a stakeholder analysis that identifies the participants and their actions, interests and objectives. That supplies the structure for further discussion on ways to combat phishing attacks in the short and long term.

### 10.1 Identifying the participants in phishing

Stakeholder analysis has been used in this chapter to obtain a better understanding of phishing. The research objective is to provide a conceptual overview of the phishing process.

The first stakeholder is the *on-line fraudster (phisher)* who uses deceptive techniques to attack organisations and consumers. According to the Anti-Phishing Working Group (APWG) the objectives of a phisher have generally been credit and debit card account numbers and PINs. The role of *government* is to legislate and enforce directives to regulate spam and on-line fraud. While governmental bodies and *anti-spam software companies* are trying to tackle spam, *organisations* can in the meantime take a proactive approach in combating the phishing threat. That includes cooperation with IT experts in order to develop stronger authentication for electronic transactions and more widespread deployment of anti-virus, anti-spam and privacy protection software. By understanding the tools and techniques which are used by cyber-criminals, organisations can prevent many of the most popular phishing attacks. *Consumers* can contribute to tackling the problem by purchasing and using anti-virus and anti-spam filtering programs, by reporting phishing scams and in general by being suspicious and verifying e-mail authenticity. Finally *anti-phishing associations* act as information providers, educators and regulators.

Table 8 shows the major stakeholders of phishing, their type of participation and actions that can be followed in the future.

*Table 8 – Stakeholder analysis for phishing*

| Phishing stakeholders | Type of participation | Actions - interests - objectives |
|---|---|---|
| **Cyber criminals** | Use of deceptive techniques (Trojan horses) and phishing methods to attack organisations and consumers. | Collection of personal information such as credit card numbers, account usernames and passwords, social security numbers. |
| **Organisations** | Receive phishing attacks that harm the brand and reduce the ability to conduct business on-line. | Protect company from phishing attacks by blocking spam and educating consumers and employees about new fraud techniques.<br>Report and share phishing fraud incidents with other stakeholders.<br>Establish corporate policies and communicate them to consumers.<br>Provide a way for consumers to validate that e-mails are genuine.<br>Monitor the internet for phishing web-sites.<br>Post warnings on the company's web-site when a phishing attack has been detected. |
| **Customers consumers** | Receive authentic-looking messages that instruct them to provide sensitive personal information.<br>Consumers cannot always detect fraudulent e-mails that appear to be from legitimate sources. | Consider purchasing and using anti-virus and anti-spam filtering programs.<br>User awareness and education is a key issue in tackling phishing attacks.<br>Report phishing scams to the companies whose web sites have been attacked by on-line fraudsters.<br>Be suspicious and verify e-mail authenticity. |
| **Technical solutions** | Prevent network intrusions and dissemination of trade secrets. | Changes in the structure of e-mail technology – Secure SMTP. Stronger authentication at web sites.<br>Fix browser insecurities. Since most phishing attacks proliferate through UCE, anti-spam technologies can be very effective at preventing the majority of phishing attacks.<br>Automatically blocking delivery of sensitive information to third parties. |
| **Government legislation** | Producing legislation to secure the e-commerce environment.<br>Ask the public to report possible phishing schemes promptly to law enforcement. | Awareness issues.<br>Receive feedback from other stakeholders about the effectiveness of legislation.<br>Cooperation with industry.<br>Develop actions in areas like complaint mechanisms, remedies and penalties, cross-border complaints, international cooperation, monitoring. |
| **Anti-phishing associations** | Provide educational and awareness-raising programmes to empower consumers to avoid giving personal information to on-line fraudsters. | Raise public awareness by informing consumers about spamming tactics and providing them with suggestions on how to block spam |

As the table suggests, there are a number of opportunities for the development of technical solutions starting from browser insecurities, to company web site security, to the transmission of personal information. In the past, password authentication has been sufficient to cover the needs of the e-commerce transactions. However, the rapid increase of on-line identity theft shows that passwords alone cannot guarantee a secure on-line environment. One of the most effective ways to tackle a phishing attack

is to make it very difficult for cyber-criminals to remotely steal users' on-line identity. SMTP is the communication protocol which is used to transmit e-mail over the internet. "The objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently" (Postel, 1982). There is no reference to security in that statement. SMTP has no built-in security measures to authenticate who is sending an e-mail. There is no guarantee that the sender of the e-mail is legitimate or that the e-mail address is not spoofed. Proposed changes in the structure of e-mail technology to assist in the reduction of spam and phishing are long-term solutions. Since these changes need time to be delivered to the internet community, phishing e-mail scams require a more urgent short-term solution. Authentication is a foundation for e-business because it establishes trust by ensuring that both sender and receiver are who they claim to be.

### 10.2 Consumer awareness and education

Consumer awareness and education complement technology in reducing the number of victims of phishing scams. In July 2004, MailFrontier launched its Phishing IQ Test (MailFrontier, 2004b) where individuals were encouraged to test their ability to identify phishing e-mails. Respondents viewed ten real-life e-mails and voted on the status: legitimate or fraud. To date, more than 190,000 individuals have tested their Phishing IQ. Approximately 30% of the responses inaccurately identify phishing e-mails as legitimate, or legitimate e-mails as phishing scams. Those results mirror findings of an earlier MailFrontier national survey fielded in July. Similarly, Issues and Answers Network found that 28% of US adults inaccurately identified a phishing scam versus a legitimate e-mail. However, consumer education is not effective all the time. Cyber criminals are devious and inventive, and as a result it is not realistic to believe that users with average internet knowledge can keep up with them.

Governments and non-governmental organisations have a joint role in raising public awareness and general education, as well as identifying perpetrators and producing penalties. For example, the Anti-Phishing Working Group (APWG) is an organisation with the objective of developing a solution to e-mail phishing (NASCIO, 2005). It uses a consortium approach in that it is composed of financial institutions, e-commerce providers, ISPs, web e-mail services, and software vendors. APWG suggests three lines of attack in combating e-mail phishing: (1) strong authentication of any users visiting a business website, such as using two-factor authentication; (2)

using enhanced DNS capabilities to verify the IP address of a sender's e-mail server, and (3) using S/MIME digital signatures to sign outbound mail and providing signature verification at the gateway or e-mail client.

### 10.3 The three-layer protection scheme

Longer-term approaches lie with companies in forming policies that can be followed in the event of such incidents, and provide assurance regarding the authenticity of their own websites. This latter action needs to be part of a discussion with technical developers and will be discussed in the following paragraph. At a policy level, the three-layer approach suggested by EnTrust (2005) can provide a useful framework. This strategy follows a logical sequence of detection, response and mitigation. At the detection level, they recommend internet monitoring for detecting identity theft attacks. It involves e-mail traffic monitoring for detecting the sending of phishing e-mails as well as web monitoring for detecting fraudulent sites. Second, at the response level, they recommend immediate action in cooperation with ISPs to shut down fraudulent sites. The final layer is to mitigate the consequences of attacks by reducing financial losses and re-establishing user confidence.

## 11. Summary and conclusions

In this chapter the extent of the spam problem has been analysed and the threat to organisations and consumers posed by a new type of e-mail fraud known as phishing emphasised. Further, ways were demonstrated in which fraud may be perpetrated, and innocent users misled by clever representations of web sites and convincing words. With the number of online scams increasing, addressing this issue has become a priority. The structure given by the stakeholder analysis is a beginning in providing a framework for thinking about the issues and the approaches that could be taken – both short-term and long-term – to address the problem.

# CHAPTER 5 TOWARD AN INTEGRATED APPROACH

The previous chapter identified the scale of the spam problem and investigated the negative impact on receivers. This chapter categorises the different players of spam using stakeholder analysis and introduces a mechanism for tackling spam.

## 1. Stakeholder analysis

There are four primary groups of stakeholders: senders of spam, receivers of spam intermediaries, and government.

- Senders of spam include corporations, direct marketers, and a host of other spammers.
- Receivers of spam include individuals and on-line users.
- Intermediaries intervene in the UCE process, directly or indirectly, to control, manage and coordinate the process, and include:
  - ISPs, who typically deploy anti-spam tools and/or e-mail usage policies for their customers;
  - direct marketing associations (DMAs), who coordinate and control their members' communication behaviours through their codes and policies, and
  - consumer privacy associations.
- Government attempts to oversee and regulate the UCE process.

***Senders of spam***

Corporations: One of the major factors that makes e-mail marketing an attractive proposition for senders is the low marginal costs for sending bulk e-mails. Several corporations solicit their customers' e-mail addresses to send them promotional and other material. Corporations use these e-mails to conduct targeted campaigns, distribute material such as discounts and coupons, and for general promotional purposes. Another positive attribute of e-mail marketing concerns the affordability by small and medium-sized businesses who are constrained by resources from conducting large marketing or promotional campaigns. An argument that has been floated in favour of e-mail advertising is that this represents a significant economic

opportunity for small and medium enterprises and it should not be undermined by restrictive regulations.

Direct marketers: This group is engaged in the business of direct marketing. They maintain customer contact databases and engage in commercial communication on behalf of other merchants and marketers. Customer contact information is usually solicited or collected by direct marketers. Many corporations and marketers tend to outsource their e-mail communication or promotional campaigns to these direct marketers, who provide e-mail and other direct marketing services. For direct marketers, the low costs of e-mail marketing are extremely attractive because even low response rates could generate profit.

Others: Other spammers include those who send e-mails without any prior consent from recipients. They collect e-mail addresses from various on-line resources such as newsgroups, online directories and web pages, and use them for sending commercial e-mails. They claim that e-mail addresses are as public as phone numbers. Those who do not want to receive junk e-mail should not place their addresses anywhere that is publicly accessible. Relying on tools such as automatic harvesting programs and dictionary attacks, spammers have developed a number of ways to collect e-mail addresses. In addition, by relying on technical measures such as false headers, mail relays and spoofing, spammers can hide their identities making them difficult to locate.

***Receivers of spam***

Consumers: The major motivator for individuals to opt in to e-mail lists is the anticipation of receiving relevant material that matches their interests. Individuals tend to value the relevance of promotional messages (Grunert, 1996; Gengler, 1995). Opted-in customers are free to unsubscribe or to leave the listing at any time. However, the real problem arises when individuals are targeted for UCE in which they have no interest or relevance. Large volumes of commercial e-mail communication tend to irritate individuals because they are forced to spend their time and effort in downloading, reading and deleting spam. Krishnamurthy (2000) lists a number of ways in which UCE could become an unethical communication practice – violation of privacy, volume of e-mails that consume time and effort, irrelevance of communication received, deceptiveness of e-mails (forging sender identity or message

title), offensiveness and targeting vulnerable customers. Individuals' privacy cost is a major factor that raises serious concerns about the privacy of the information that they provide to companies and marketers. Finally, individuals tend to favour mailing lists that have clear and reliable opt-out opportunities.

When individuals receive spam at work, it creates problems for their employing organisations as well. Enterprises play a double role in the UCE process. When employees are targeted for UCE, the precious server space and bandwidth of the corporate IT infrastructure gets wasted. Moreover, the problem of dealing with spam rests on the shoulders of organisations as it poses a threat to employee productivity as well as to organisations' security and privacy. While most firms do not wish to receive any unsolicited e-mail communication from third parties, most of them use e-mail themselves as a marketing tool. Firms need to invest in anti-spam tools to control incoming spam, but need to strike a delicate balance with their own e-mail marketing campaigns.

***Intermediaries***

Internet Service Providers (ISPs): An important stakeholder in the UCE process is the ISP, who provides internet access services to both senders and recipients. ISPs have become critical components of the commercial internet providing customers internet access, web hosting services, e-commerce technologies, and e-mail access.

According to the Electronic Commerce (EC Directive) Regulations 2002, ISPs are "mere conduits" and as a result are not liable for the content of information they transmit through their networks. There is nevertheless a general agreement that ISPs need to be the first line of defence in combating spam. The Internet Engineering Task Force's (IETF) Network Working Group has developed protocol standards (RFC 2871) and best practices (RFCs 2505 and 2635) for ISPs to follow in order to help reduce spam. (RFC = request for comments.) These standards require ISPs to prevent their mail servers from being used by unauthorised third parties to relay e-mails, and to provide sufficient information in e-mail headers to make it possible to verify the sources of e-mail.

Direct Marketing Associations: Associations of direct marketers are also trying to control their members' behaviour on-line (Direct Marketing Association, 2002). But

even effective self-regulation by such bodies may be ineffective, as many spammers may not be members. For instance, the Canadian Marketing Association (CMA) has established for its members a code and guidelines dealing with internet use for the distribution of promotional materials. Under this code, consumers who are solicited must be given the opportunity of opting out of any further communication from the marketer. A marketer who fails to live up to the CMA code is expelled from the Association.

Consumer Privacy Associations: Their role is to provide education and awareness-raising programs to empower consumers to make informed choices in relation to spam-reduction strategies and technologies. For example the Korean Information Security Agency has set up a black list of spammers, while the Union Fédérale des Consommateurs de Quimper in France provides information on existing spam-related laws and how to take legal action against spammers. In other cases, they operate as reporting centres that receive complaints on spam, and analyse or forward spam to the appropriate authorities for further investigation.

***Government***

More and more countries have laws in place that directly or indirectly regulate spam. Anti-spam laws generally impose labelling requirements, prohibit the transmission of commercial communication without the consent (opt in/out) of recipients, and ban the use of spamware. Examples of regulations across the globe include the Canadian Code of Practice for Consumer Protection in E-Commerce, the US Can-Spam Act of 2003 for UCE, and other similar regulations by the EU. Legislation usually relates to a number of issues:

- Breach of contract with the ISP: the spammer may breach the terms and conditions of his ISP by sending bulk UCE.
- Trademark infringement: forged headers (e.g. AOL trademark).
- Computer Misuse Act: malicious program code integrated within the e-mail.
- Data Protection Act 1998: impinging on personal information. A data controller (in this case spammer) must process data fairly and lawfully.
- Consumer law: deceptive on-line offers and insecure e-commerce environment.

Figure 2 summarises the different positions discussed in this chapter and provides a pictorial representation of the key stakeholders in the UCE process.

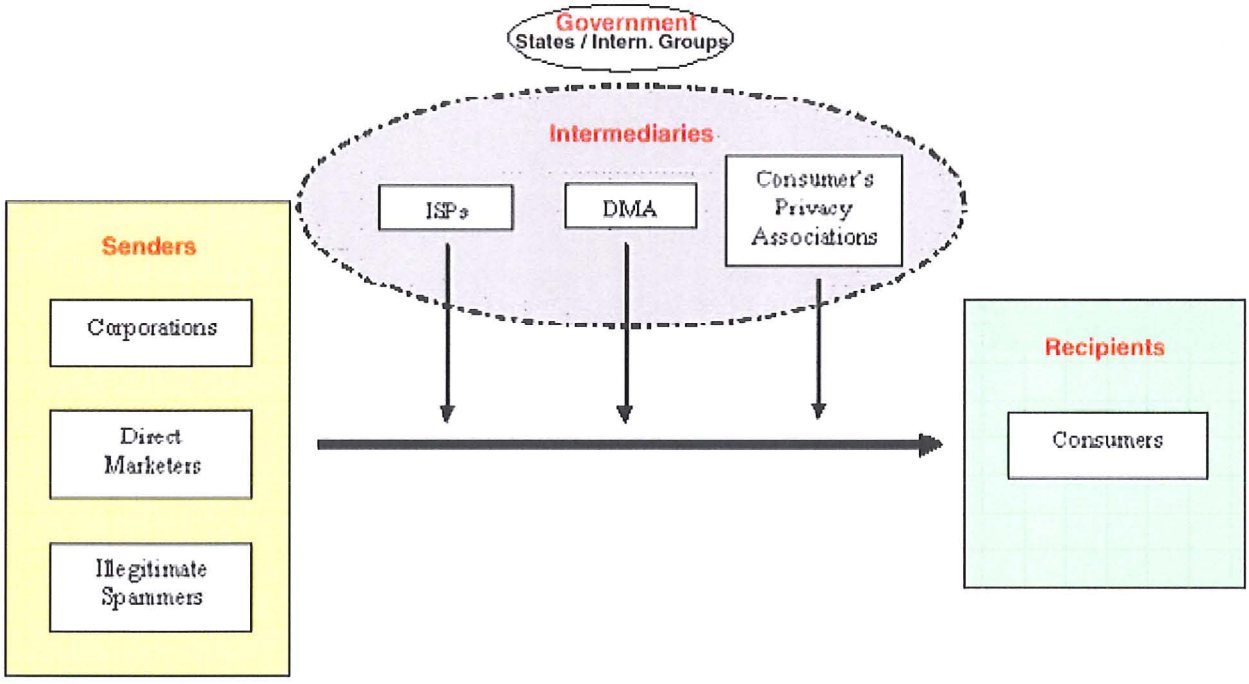



*Figure 13 – Key stakeholders in the UCE process*

## 2. Mechanisms for tackling UCE

Customer pressure could be a powerful force that goes a long way in containing and eliminating spam. The customer pressure for better on-line services including spam-free e-mail communication will force ISPs to develop anti-spamming software applications and enforce constructive e-mail policies. If ISPs do not comply, they will face the danger of being excluded from the market by customers. There are a number of actions individuals can take when receiving UCE.

1. Disregard and delete. Simply delete the message. This is an acceptable solution as long as the amount of spam is small. However, it is not a recommended method when spam reaches a high rate.
2. Block and delete. This is a more effective method since blocking will not allow further receipt of communication from the same source. However, it contains the danger of legitimate e-mail being wrongly blocked.
3. Quarantine. There are several anti-spamming products that quarantine suspicious e-mail and put it in a separate folder for further inspection.

4. Report. Report all spam messages to an appropriate authority (ISP or possibly the police) although it may not lead to the identification of the spammer.
5. Respond. There are cases where the commercial e-mail message is coming from a known source or from a trusted third party and then we may read it, download an attachment or even reply. Although it is not recommended, individuals may receive commercial communication that is close to their interest and as a result open the message.

Table 9 presents our initial typology of UCE, along with key stakeholders in each category and possible response mechanisms for minimising spam:

***Table 9 – Mechanisms for containing UCE: stakeholders and potential responses***

| | | | | |
|---|---|---|---|---|
| **Without consent** | | | **Key stakeholders**<br>DMAs<br>ISPs<br>Consumer privacy associations<br>III<br>**Potential responses**<br>Enforcement of code of conduct by DMAs.<br>White and black listing by ISPs.<br>Promote consumer awareness on privacy issues. | **Key stakeholders**<br>Government<br>ISPs<br>IV<br>**Potential responses**<br>Anti-spam legislations.<br>Penalties for non-compliance with legislation. |
| **With consent** | **Key stakeholders**<br>Consumers<br>Corporations<br>I<br>**Potential responses**<br>Consumer opt-in/out.<br>Explicit policies by corporations | **Key stakeholders**<br>DMAs<br>ISPs<br>II<br>**Potential res**<br>Enforcing code of conduct by DMAs.<br>E-mail usage policies and filtering solutions by ISPs. | | |
| | **Low potential negative impact** | | **High potential negative impact** | |

Type I: This type of UCE is relatively easy to manage and control. The key stakeholders in this type of communication are customers and corporations. The UCE here is similar to the idea of permission marketing (Godin, 1999), where the explicit permission of customers is sought before communications are sent to them. Along with permission, possible compensation, rewards, volume and targeting are also

considered (Milne, 1993). Consumers could opt in or opt out of UCE, or they could use software tools to monitor, delete or respond to a communication. Thousands of corporations (Easyjet, Expedia, Amazon) who collect customer e-mail IDs have explicit policies in place that specify the purpose of collecting the contact information and how this information will be used.

Type II: The key stakeholders here are the DMA and ISPs as this kind of UCE is third-party-initiated, rather than customer-initiated. The DMA forms an umbrella organisation for most direct marketers who are governed by the code of conduct and norms prescribed by the DMA. The DMA's interest lies in protecting the efficacy of e-mail marketing as a promising and cost-effective marketing medium. Another important stakeholder group, who can play a critical role in minimising this type of UCE, is the ISP, who can adopt stringent measures toward those responsible for sending and propagating spam. ISPs represent a fairly large industry across the globe, and the policies adopted by ISPs vary considerably. While some ISPs may be effective in controlling spam, others may not have stringent measures in place. ISPs could enforce strict anti-spam policies for their members, in addition to deploying anti-spam filtering solutions.

Type III: This category includes cases where customer opt-out mechanisms are not effective, or cases where the e-mail lists have been passed on to different parties with or without the explicit knowledge or consent of the customer. The key stakeholders who can be effective in controlling this type of communication are DMAs, ISPs and Consumer Privacy Associations. DMAs could ensure member compliance with rules and norms on information sharing and with codes of practice. ISPs set up and maintain black/white lists that control the flow of e-mail communication. The purpose of a white list is to specify elements whose inclusion in an e-mail guarantee it will pass the filter and be delivered. On the other hand, inclusion in a black list blocks the passage of e-mail. Consumers' Privacy Associations provide educational programmes and awareness campaigns to empower customers to make informed choices in relation to spam-reduction strategies and technologies. They also operate reporting centres that receive complaints about spam, and analyse or forward spam to the appropriate authorities for further investigation

Type IV: This represents the most dangerous form of UCE, where very little is known about the origin of the UCE, with potentially high negative impacts. While a number of technological solutions in the form of advanced filtering tools, anti-spam and anti-

virus solutions have become available in the marketplace, none of them have been completely successful in eliminating spam. The key stakeholders in this type of communication are ISPs and governments. While ISPs can effectively implement sophisticated technological solutions, governments should propose and enact anti-spam legislation to combat UCE. Government deals with issues such as prevention, consumer awareness, reporting mechanisms, remedies and penalties, cross-border complaints, international cooperation and monitoring.

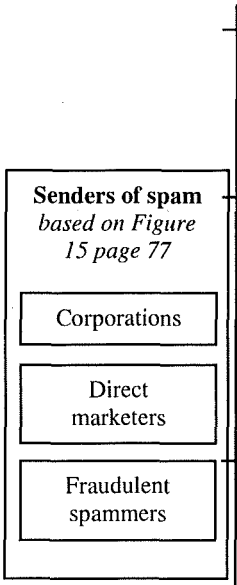
Arguments have been made for and against legalising UCE through legislation. The US Can-Spam Act requires that spam e-mails include a valid return e-mail address, a postal address for the sending company, a working opt-out mechanism, and a relevant subject line. This law does not prohibit senders from sending spam messages until customers explicitly ask to be opted out. Can-Spam is an opt-out legislation that puts the onus on individual users to let marketers know that they do not wish to receive UCE. In contrast, the EU and the UK use opt-in legislation where on-line marketers can send UCE messages only to those consumers who have given their prior consent to receive them, except where users are current customers of a particular company.

There are also differences in the interpretation of regulations across nations and even within groups of nations such as the EU. While some impose fines for unsolicited e-mail sent to both customers and businesses, others only penalise spam sent to customers. There are a number of differences among EU member states in areas such as the nature of consent (oral or written), explicit or implicit, active versus passive, and the authorities who would manage the opt-in/out lists. Spain takes the view that messages can only be sent to those who have authorised them, but Denmark has banned the sending of messages unless the recipient has actually requested them. In the UK, participation in a draw would constitute consent to receive further e-mails. Though harmonisation of laws across a larger group of nations worldwide is a formidable task, efforts are in progress toward achieving this larger goal.

Apart from legislation, there are several steps that can be taken by corporations and individuals to combat UCE. One of the key steps that businesses can adopt is development of an e-policy that clearly details how spam is handled. E-policies need to specify how employees should handle unsolicited e-mail, especially if the e-mail contains offensive material. In addition, an e-policy should detail how employees can use e-mail for personal use. Ensuring that employees understand and acknowledge e-policies is essential. A well structured e-mail policy, along with educating

employees and enforcing compliance with the formulated policies using technological tools, can go a long way in combating UCE in the workplace. Increasing consumer awareness globally is another key measure that could help address the problem of UCE. Consumers need to be aware of their rights, privacy issues, and mechanisms with which they can combat spam. The proposed integration of approaches involves communication among stakeholder groups, both in developing better defences against spam and in implementing those defences. The following table combines the initial typology of UCE, along with key stakeholders in each category and possible response mechanisms for minimising spam; it also provides a pictorial representation of the key stakeholders in the UCE process.

***Table 10 – How to tackle spam: the integrated scenario***




| Type of spam *based on Table 6 p58* | Key stakeholders/role *based on Table 9 p 78* | Potential responses *based on Table 1 p44 / Table 9 p 78* |
|---|---|---|
| **I** The recipient provides explicit consent to receive direct e-mail marketing | **Consumers** *Recipients of UCE*<br>**Organisations** *Receivers/senders* | Consumer opt-in/out. Use of anti-spam technology. User awareness.<br>Organisations develop corporate e-mail policies. |
| **II** Indirect, permission-based partnership | **DMA** *Co-ordinators*<br>**ISPs** *Develop, regulate, monitor* | Develop and enforce codes of conduct and acceptable e-mail policies for commercial communication. Develop technical anti-spam solutions. |
| **III** Spam that originates from third parties without explicit permission or consent of recipients | **Consumer's Privacy Associations** *Provide information,, regulate, educate*<br>**DMA** - *Co-ordinate (see above)*<br>**ISPs** - *Develop, regulate, monitor (see above)* | Provide educational and awareness-raising programmes to educate consumers in relation to spam reduction strategies and technologies. Operate reporting centres that receive complaints on spam |
| **IV** The identity of senders is unknown. Potentially harmful to the recipients. | **Government** *Legislate/enforce*<br>**ISPs** *Regulate, monitor (see above)* | Penalties for non-compliance with legislation. Harmonisation and effective enforcement of the legislation across countries. Cooperation with industry consumer awareness. |

The above diagram shows the link between the stakeholders identified in Figure 13 and their distinctive role within the UCE context (Table 9), together with how each stakeholder could positively address the spam problem. By combining the elements identified in the previous tables it can be seen that all stakeholders have a part to play in reducing spam, thus upholding the concept of an integrated approach.

# CHAPTER 6 ANTI-SPAM LEGISLATION

## 1. Introduction

One of the major stakeholders in addressing spam is government, which produces legislation to secure the e-commerce environment from threats such as spam, viruses, on-line fraud, cyber pornography and paedophilia. Legislation itself cannot resolve the problem of spam, however. Governments are also responsible for implementation and enforcement issues, self-regulatory and technical issues, and awareness issues.

The current chapter provides an evaluation and comparison of a number of different legislative approaches, leading to a better understanding of how legislation has developed and how it affects other spam stakeholders. The chapter will conclude that legislation is only a part of the proposed anti-spam integrated scenario.

## 2. The need for anti-spam legislation

So far the research has shown that spam is responsible for the dissemination of viruses and that there is a direct relationship between spam and cyber crime or phishing (discussed in Chapter 4). The increasingly sophisticated variants of spam and the threats they pose have brought anti-spam measures to the forefront of the attention of government agencies, consumer groups and businesses worldwide. Given the severity of the issue and the potential damages spam can cause, legislative measures have been implemented to control and possibly eliminate spam. Spammers may not be unduly obstructed by anti-spam legislation since they can change their tactics or simply move their servers to locations that that do not have anti-spam regulations. However, action against spammers need not be totally ineffective. According to Spamhaus (an independent network which tracks spammers, spam gangs and spam services), 80% of spam received by internet users in North America and Europe is sent by a hard-core group of fewer than two hundred spam outfits, comprising some five to six hundred professional spammers (Spamhaus, 2004b). Therefore, it is possible to identify and control this core group of spammers. By effectively deploying legislative tools, it may be possible to penalise, control and minimise spamming.

## 3. Types of liability

Anti-spam legislation refers to civil and criminal sanctions, including sizable fines and possible imprisonment for spammers. The civil penalties found in anti-spam legislation are particularly noteworthy since they frequently provide the right to stakeholders, such as ISPs or on-line consumers, to bring private actions to obtain statutory damages. The term "spam violation" means committing a number of breaches prohibited by a country's commercial e-mail laws, including but not necessarily limited to:

- sending commercial e-mail communication containing deceptive content;
- sending commercial e-mail without providing the recipient the opportunity to opt out with a means such as a valid return e-mail address or an internet-based mechanism;
- sending commercial e-mail that contains misleading information about the sender of the message or fails to disclose the sender's address, and
- sending commercial e-mail when the recipient has specifically requested the sender not to do so.

More specifically a spammer can be held liable for some of the following reasons.

- ***Contractual liability***

  By sending unsolicited commercial e-mails, a spammer may breach the terms and conditions of his ISP causing damage of a nature described above.

- ***Liability deriving from Article 7 Data Protection Act 1998***

  Article 7 of the Data Protection Act states that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

  Since electronic mail addresses, other than business addresses, are deemed to be personal information, the legislation will impose some restrictions and obligations on how these addresses and other personal information are collected, used and disclosed in the course of commercial activity by the data controller (in this case the spammer). The law also creates an obligation on ISPs and others

who store electronic mail addresses to provide appropriate security for this personal information. Individuals or organisations buying, selling or leasing electronic mailing lists will be subject to the provisions of the legislation, if these transactions take place across provincial and national borders.

Spammers may also hack the do-not-spam registry and sell the e-mail addresses to other spammers. These addresses would be more valuable than harvested addresses because they would be valid addresses and would presumably reach a large number of busy professionals and other decision makers, who typically do not put their e-mail addresses on the web.

- ***Theft of personal information***

  Fraudulent e-mail messages are messages that appear to be sent from a legitimate company web-site or domain address, but in fact are not. In reality, spammers are hijacking the company's brand to attract the attention of customers and potential customers, often to gain information. Harvesting of e-mail addresses of customers may result in a breach of confidential information, for which a claim by the customer may be brought. As described in Chapter 4, spam and viruses are closely associated. More than 98% of computer viruses now arrive via spam, cleverly camouflaged with introductory messages or tempting picture attachments. A virus is malicious program code that can take the form of a Trojan horse. Apparently it can be harmless, but it can get control of a recipient's computer and steal credit card details and other personal information.

## 4. A review of anti-spam legislation

The evasive and pervasive nature of spam, as well as its negative impact on consumers and e-commerce, has forced governmental bodies into trying to deal with the problem. Nations have enacted different kinds of laws to control spam. The following table provides an overview of the anti-spam legal environments in the EU, Australia, Canada, the USA, Japan and New Zealand.

*Table 11 – Anti-spam legal environment*

| Country | Legislation – anti-spam statutes |
|---|---|
| Australia | - Spam Act of 2003<br>- Telecommunications Act of 1997<br>- Australia Parts IVA, V, and VC of the Trade Practices Act of 1974 |
| Canada | - Personal Information Protection and Electronic Documents Act (PIPEDA)<br>- Competition Act.<br>- Charter of Rights and Freedoms<br>- The Criminal Code and the Competition Act<br>- Canadian Code of Practice for Consumer Protection in E-Commerce |
| EU | - Privacy and Electronic Communication Regulations 2003 (UK)<br>- Data Protection Act of 1998 (UK)<br>- Electronic Commerce Regulations of 2002 (all adapted from EC Directives, e.g. Directive on Privacy and Electronic Communications 2002/58/EC) |
| Japan | - The Law on Regulation of Transmission of Specified Electronic Mail July 2002<br>- Specific Commercial Transactions Law, 2002 |
| New Zealand | - Has not yet enacted legislation to regulate spam. In progress. |
| USA | - Can-Spam Act of 2003<br>- Laws enforced by the Federal Trade Commission<br>- Section 5 of the Federal Trade Commission Act |

## 4.1 EU and UK legislation

### 4.1.1 Key elements of the EU Directive

In the EU, although the negative effects of spam were recognised, the question remained whether the sending of spam was a legitimate activity. UK law (UK Anti-spam Law, 2003) largely follows the EU Directive (EU Directive 2002/58/EC, 2002). In July 2002, the European Parliament and Council voted to ban spam. The directive specifies the following.

> (40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them.

This directive means that people have to opt in or specifically place a request to receive commercial e-mail. Under Article 13 of the Directive, the use of e-mail and SMS (text message to mobile phones) for direct marketing will only be allowed in case of those customers/subscribers who have given their prior explicit consent. Thus the Directive places e-mail marketing on the same footing as unsolicited faxing and automated telephone systems. The term "opt in", in the context of receiving

unsolicited commercial e-mail, is limited by "for the time being". It is not specifically defined in the regulations, but it implies that the consent has a transient nature and the guidance makes clear that the consent will remain valid until it has been specifically withdrawn or it is otherwise clear that the recipient no longer wishes to receive marketing commercial communications.

> (41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/E.

The Directive makes an exception where there is an existing customer relationship and the supplier has obtained the customer details in the context of a sale of goods or services. In this case, the supplier may use the customer details for the purpose of direct marketing in relation to its own similar goods or services.

> (41) When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

The customer must be clearly and distinctively given the opportunity to object, free of charge and in an easy manner, to the use of the e-mail address when collected, and on the occasion of each message in case the customer has not initially refused such use. This exception leaves open to interpretation whether goods or services advertised are similar to those previously purchased. Moreover, it seems from the wording that the exception only applies where there has been an actual sale rather than for example an enquiry. It also appears that only the party that obtained the details can use them. For instance, a manufacturer cannot send e-mails to customers whose e-mail address was obtained by a retailer. The term "similar products and services" is related to soft opt-in. That means that a product or service can be offered only during the negotiation period or if it is similar to those offered in the marketing e-mail communication.

> (43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes

The Directive also prohibits sending direct marketing e-mails that disguise or conceal the identity of the sender or are without a valid address to which the recipient may send a request that such communications cease.

### 4.1.2 Effectiveness of the EU Directive

- ***Implementation issues***

  The implementation of the EU Directive differs between the member states. While some impose fines for unsolicited e-mail sent to both customers and businesses, others only penalise in the case of spam sent to customers. Also the term "opt-in" is open to interpretation. More specifically, some national laws (e.g. Spain) had already introduced an opt-in regime for e-mail before the Directive of 2002. Some member states "transposed" the Directive into national law but modified the concept of opt-in (e.g. Denmark), and others transposed it only partially (e.g. Belgium). Finally, a large number of member states transposed the Directive as late as summer 2004 (e.g. France and Germany). Spain takes the view that messages can only be sent to those who have given their authorisation, but Denmark has banned the sending of messages unless the recipient has actually requested them. In the UK, participation in a draw would constitute consent to receive further e-mails. The Information Commissioner in the UK notes that "harmonisation among the member states is the desirable objective but also a very difficult task" (Jones, 2003).

- ***Distinction between individual and corporate subscribers***

  There are a number of divergences among member states such as whether the Directive applies to natural and/or legal persons. And whether the requirements for consent are oral/written, explicit/implicit, active/passive and who manages the opt-in/out mailing lists. The distinction between individual and corporate subscribers is an important issue, since the use of e-mail and SMS for direct marketing is only allowed in respect of subscribers who have given their prior explicit consent. The definition of "individual" covers traders such as consultants who run their businesses on their own rather than under the umbrella of a company. When the recipient of commercial communication is a partnership subscriber, the question is raised as to whose consent is required. Strictly speaking the legislation states that the consent of the individual

recipients or persons should be obtained. However, the UK Information Commissioner recognises that there are circumstances where the wish of the organisation to receive marketing materials may override the wishes of individual employees. Therefore, marketers may obtain consent from a single person who acts on behalf of the partnership to receive commercial communications. Finally, marketers should ensure that they comply with the principles of the Data Protection Act 1998.

- ***The applicability of the anti-spam legislation within the EU***

  There are also practical questions that the EU Directive has not explicitly addressed, such as which law is applicable if a UK-based company sends unsolicited e-mail to Italy or vice-versa. According to the UK Information Commissioner, if both sender and recipient are companies, sending spam is not illegal. If the recipient is an individual he can complain to the sender's ISP or to the Direct Marketing Association. The recipient in Italy may also sue the sender in the UK and the action will be heard in the UK. Szabolcs Koppanyi (Koppanyi, 2003) of the European Commission agreed that the EU needs to find a common forum for exchanging views, and explained that a process is being put in place within the European Commission for investigating the following elements of the Directive: remedies and penalties, complaints procedures, cross-border complaints, cooperation with third countries, monitoring, contractual arrangements, codes of conduct, acceptable marketing practices and out-of-court redress. The European Contact Network of Spam Authorities (CNSA) was established for that purpose in 2004.

- ***Effectiveness of transition rules***

  Transition rules for adopting the new legislation have often been left out, creating a "grey zone" for both companies and customers. Many legitimate companies use e-mail newsletters to communicate with their customers, and in several cases this type of communication dates as far back as the 1980s. Since it is hard to prove which recipients have opted in, the question arises whether companies have the right to send a single e-mail message to existing subscribers to inform them that they must take action to confirm their subscription, or whether they have to stop all types of sending. In the event that they decide to

stop all types of sending they could be faced with an avalanche of phone call requests from confused customers asking why they do not receive newsletters anymore.

## 4.2 US legislation – Can-Spam Act 2003

According to the 2003 United Nations Conference on Trade and Development (UNCTAD) E-Commerce and Development Report, currently over 58% of all spam e-mail messages originate from the USA. Therefore, it is only natural that the US spam-related legislation is of considerable interest to the rest of the world. (UNCTAD, 2003a). The US Bill was signed by the President on 16 December 2003, and took effect on 1 January 2004 (Can-Spam Act, 2003). The purpose of the Act is to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the internet.

### 4.2.1 Key elements of the US legislation

The Can-Spam Act of 2003 represents a compromise between the various spam stakeholders, and allows e-mail marketers to send UCE unless and until the consumer opts out from receiving future messages. It also requires e-mail marketers to identify UCE as advertisements, as well as to include warning labels on UCE that contains sexual material.

Section 5

(a) Requirements for transmission of messages

(1) It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message ...that contains..... header information that is materially false or materially misleading.

(2) Prohibition of deceptive subject headings ...

(3) Inclusion of return address ...

(5) Inclusion of identifier, opt-out, and physical address ...

The new law calls the Federal Trade Commission (FTC) to study the feasibility of a Do-Not-Spam List of e-mail addresses, and prohibits spammers from disguising or hiding their identities. Spammers must also include an opt-out option in their messages. It also requires that commercial e-mail should include the sender's valid physical address, and that recipients must be given an opt-out method. Convicted spammers could face penalties of up to five years in prison.

(A) It is unlawful for any person ...

(i) the electronic mail address of the recipient was obtained using an automated means from an Internet website

(ii) the electronic mail address of the recipient was obtained using an automated means that generates possible electronic mail addresses by combining names, letters, or numbers into numerous permutations.

The Can-Spam Act prohibits address harvesting and dictionary attacks. Many spammers use automated software to collect e-mail addresses through the internet by searching web sites, newsgroups, mail lists or other on-line resources that could possibly contain e-mail addresses.

(2) to use scripts or other automated means to register for multiple electronic mail accounts

(3) to relay or retransmit a commercial electronic mail message ... without authorisation

The Can-Spam Act makes it illegal to use automated techniques such programming scripts to sign up for e-mail accounts for the purposes of sending unsolicited commercial e-mails.

S. 877—6

(b) PENALTIES — the punishment for an offense under subsection (a) is

(1) a fine under this title, imprisonment for not more than 5 years...

(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorised access to a computer system;

(2) a fine under this title, imprisonment for not more than 3 years, or both, if—

(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

(D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period;

The US anti-spam law makes it a crime (SpamLaws, 2003), subject to five years imprisonment, to send fraudulent e-mail using standard spam tactics such as false headers and misleading subject lines, and provides for civil penalties up to $11,000 per violation. Additionally the Congress gave the FTC a list of tasks such as issuing a regulation requiring that any spam containing sexually oriented material must include the warning "SEXUALLY-EXPLICIT" in the subject line (CBC News, 2004).

### 4.2.2 Can the Can-Spam Act reduce spam?

- ***Positive impact***

  The Can-Spam Act set out to reduce unsolicited e-mail by targeting the fraudulent use of third-party computer systems to relay e-mail messages, as well as messages that are unsigned or have fraudulent return addresses. It also requires all e-mail messages to include opt-out functions. The Act will indeed assist in some way to tackle the problem of spam. It makes illegal the use of open proxies or the use of false headers. To circumvent legislation, US spammers will now have to send out e-mails from their own identifiable IP addresses, rather than stealing third-party relays and proxies.

  However the new US law may not entirely stop spam. As described above, the legislation takes an opt-out approach. The big concern regarding the opt-out mechanism is that it gives the right to spammers to send spam. That means that corporate IT managers are going to keep the anti-spam filters at the mail gateway, blocking the flow of now legal but still unsolicited e-mails (Sturdevant, 2003). Several negative comments were addressed at the "Spam and the Law" conference in San Francisco on 22 January 2004 about the effectiveness of the Federal Can-Spam Act. Many professionals in the technical and legal areas have questioned the federal government's ability to enforce those restrictions, and have criticised the way that the Act supersedes stricter state laws (Amit, 2003).

- ***Do-Not- Spam Registry***

  Regarding the national do-not-spam registry, the FTC Chairman Timothy Muris, during a press conference in June 2004, stated that without an effective system for authenticating the source of e-mail any efforts to develop a registry of individual e-mail addresses will fail (Grabarek, 2004). Most spammers who already violate the anti-spam laws would ignore the requirements not to send unsolicited commercial communication to e-mail addresses that are in a do-not-spam database. Spammers might even use the do-not-spam registry as a source of valid e-mail addresses to spam further (Hailey, 2004).

- *Enforcement issues*

  Since law is only as good as its enforcement, no change will be seen in the level of spam until enforcement happens. Though the new legislation has been gradually enforced in all the US states, it overrides stricter spam punishments set by some states. In California, for example, Senator Debra Bowen's bill would have cost spammers $500 per unsolicited e-mail. The new federal anti-spam bill may not be as effective for California, or for Delaware, which were closer to developing more effective anti-spam legislation. Both California and Delaware had specified that bulk commercial communication could only be sent to recipients who had opted in to receive it. Also, California's law would have provided a way for individuals to sue offenders. The Federal legislation does neither of those things since it is only up to the government agencies and ISPs to pursue spammers. Unfortunately, the Federal legislation will create a kind of bulk unsolicited commercial e-mail that is legal under their own rules.

## 4.3 Australia – Spam Act 2003

### 4.3.1 Key elements of the Australian legislation

The Australian government has taken a strong position in relation to spam. In December 2003, it introduced legislation which bans commercial and private spam and the harvesting of e-mail addresses. The Spam Act of 2003 (Australian Government, 2003) sets up a scheme for regulating the sending of UCE, but the Bill also contains rules regulating the sending of general commercial electronic messages no matter whether or not they are unsolicited. In general the Australian government's approach to combating spam includes combining domestic legislation with international cooperation, public education, and the development of industry codes of practice and of technical counter-measures (OECD, 2004).

Section 16

Unsolicited commercial electronic messages must not be sent

The Spam Act covers electronic messages of a commercial nature such as e-mails, mobile phone text messages (SMS), multimedia messaging (MMS) and instant messaging (iM). However, the Act does not cover voice or fax telemarketing. Under the Spam Act 2003 it is illegal to send, or cause to be sent, "unsolicited commercial electronic messages" that have an Australian link. A message has an "Australian link"

if it either originates or was commissioned in Australia, or originates overseas but has been sent to an address accessed in Australia. A message should only be sent to an addressee when that person has consented to receiving it (opt-in). Those who persist in sending spam are subject to penalties up to $1.1 million for a single day of infringements.

Section 17

Commercial electronic messages must include accurate sender information

Section 18

Commercial electronic messages must contain a functional unsubscribe facility

In addition to banning spam, the Spam Act lays out rules for sending legitimate commercial electronic messages. Commercial electronic messages should contain:

- accurate information about the sender of the message; and
- an easy way for the recipients to opt-out (unsubscribe) from future mailings.

Sections 20, 21, 22

Address-harvesting software and harvested-address lists must not be supplied, acquired or used.

It is not allowed to use harvesting software for scanning electronic addresses, or lists which have been generated using such software, for sending unsolicited commercial electronic messages.

### 4.3.2 Effectiveness of the Australian legislation

Australia has been successful in modifying the behaviour of spammers and getting them to leave the jurisdiction. It aggressively requires opt-in requirements and bans tools for harvesting addresses. According to Spamhaus, the Australian anti-spam legislation is the world's best anti-spam law to date, and since its implementation Australian spammers appear almost to have ceased activities or to have left the country (Spamhaus, 2004b).

One of the key reasons why the Australian legislation is effective is that the major objective was not to prosecute spammers but to combat spam by deterring them with serious penalties and to implement an effective enforcement regime. The penalties are sufficient to provide a disincentive to any spammer located in Australia. Even if the spammer moves his operations outside Australia he will not be able to escape,

because the Anti-Spam Law includes a ban on people being "knowingly concerned in" the spam and will catch anybody knowingly involved in conducting actions, such as planning, funding or providing facilities for spam.

While in general international enforcement is a difficult task the Australian law also bans spam to Australia coming from third countries. The tough Australian anti-spam legislation sent a powerful message to spammers that the sending of unsolicited electronic junk mail will no longer be tolerated in Australia. The Spam Act 2003 hit unscrupulous spammers with penalties of up to $1.1 million for each day they send messages which break the law, while providing clear guidelines so that legitimate businesses can conduct marketing activities over the internet. The Act has required over two hundred Australian businesses to "amend their practices to comply with the Act": five of those businesses were fined for "substantial breaches", three received formal warnings, and one gave an enforceable undertaking.

Court action is being taken against an alleged global spammer in the Federal Court in Perth in the matter of *Australian Communications and Media Authority v Clarity1 Pty Ltd and Wayne Robert Mansfield* (Federal Court of Australia, 2006). From 10 April 2004 Clarity1, an Australian company, periodically sent UCE messages to electronic addresses which it had harvested from the internet using address-harvesting software, or which it had purchased from organisations or persons selling lists of electronic addresses harvested from the internet. ACMA (Australian Communications and Media Authority) alleged that Clarity1 sent 270,305,474 UCE messages (of which 74,996,560 were successfully sent) to 7,956,457 unique electronic addresses. The UCE messages sent by Clarity1 contained an unsubscribe facility, and the evidence was that some 166,000 requests to be removed from the lists were made, all of which were acted upon. Over the same time period only 79 complaints concerning UCE messages from Clarity1 were made to ACMA. ACMA alleged that Clarity1 contravened sections 16 and 22 of the Spam Act. More specifically the Australian Court found Clarity1 liable, resulting in an A$5.5m (£2.2m) fine for the following reasons.

- Section 16(1) of the Spam Act provides that a person must not send a commercial electronic message that has an Australian link.

- Section 16(2) provides a defence if the relevant electronic account holder consented to the sending of the message.
- Section 22(1) of the Spam Act prohibits the use of address-harvesting software or a harvested-address list.

This decision was significant for e-mail marketers for the following reasons.

- The inclusion of an unsubscribe facility does not impose an obligation on the recipient to reply to avoid an inference of consent.
- A business relationship cannot be inferred if the communication is one-sided.
- Consent cannot be inferred from the mere fact that the relevant electronic address has been published.
- The Spam Act prevents the use of harvested lists from the date the Act came into operation, regardless of when the lists were compiled.

#### 4.3.3 Spam and internet security information/education programme

The Australian government understood the importance of information and education for the on-line community. For that reason it has developed web portals that contain information for consumers and businesses about compliance with the Spam Act, reducing the amount of spam they receive, boosting internet security, avoiding e-mail scams, protecting children online, making a spam report or complaint, and the steps the Australian government is taking to combat spam (Consumer Guide, 2003).

### 4.4 Anti-spam legislation in Canada

#### 4.4.1 Key elements of the Canadian legislation

***Competition Act***

In Canada many stakeholders expressed the view that improving the enforcement of existing Canadian laws could have a significant impact on reducing the flow of spam. Distribution of unsolicited promotional and product information, in print form or over electronic networks, is not illegal nor is it regulated in Canada. In the same way, advertising, except in the Canadian broadcasting system, is generally not federally regulated. There are, however, specific provisions in various laws dealing with such things as tobacco advertising or misleading advertising in the Competition Act.

***Charter of Rights and Freedoms and Telecommunications Act***

Spam is also considered a form of expression and, as such, any attempt by the government to control it, regardless of the means, would have to be consistent with section 2 of the Charter of Rights and Freedoms. ISPs are subject to the same laws and regulations as most other businesses and there are no special rules for the internet service industry. Unlike the telephone companies, ISPs are generally not subject to regulation under the Telecommunications Act because they are not considered to be facilities-based common carriers.

***Personal Information Protection and Electronic Documents Act (PIPEDA)***

In addition Canada's private-sector privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), (Department of Justice Canada, 2000), is a powerful legal tool for challenging a Canadian spammer on privacy grounds. Once a spammer is caught within the PIPEDA framework, the statute could be used to prohibit the collection of personally identifiable e-mail addresses through harvesting techniques, to require opt-in consent in certain circumstances, and to ensure that organisations honour opt-out requests. Under this Act, as of January 2004, commercial bulk e-mailers who establish or acquire lists of e-mail addresses must ensure that recipients have given some form of consent to commercial solicitation. This law also specifies that e-mail addresses can only be used for the purpose for which they are collected, and that the owners of these e-mail addresses must consent to any secondary use.

***The Criminal Code***

Sending unsolicited commercial e-mail for a legal product or service is currently not a criminal offence. Like unsolicited commercial information distributed through traditional mail, it can be considered a form of advertising and marketing. However Canada's Criminal Code could also be used to take action against certain spamming activities. Section 380 of the Code, which covers fraudulent conduct, could be interpreted to cover spam that contains fraudulent or false content. Several e-mail abusers now resort to forged information in electronic mail headers to avoid being identified, and to sending Trojan programs embedded in e-mail messages that can be activated by spammers to relay spam. Such methods of gaining unauthorised access to computer systems violate several current provisions of the Criminal Code. These

provisions provide for substantial fines and even imprisonment. Furthermore the Code could also be applied to spamming organisations that make unauthorised use of e-mail servers without permission to send spam. In addition the relevant provision could also include e-mail harvesting (Department of Justice Canada, 2002).

***Canadian Code of Practice for Consumer Protection in Electronic Commerce***

In 2003 the Working Group on Electronic Commerce and Consumers developed the Canadian Code of Practice for Consumer Protection in Electronic Commerce Preface (Canada's Business and Consumer Site, 2003) based on the Principles of Consumer Protection for Electronic Commerce. The Code is consistent with the Organisation for Economic Cooperation and Development's Guidelines for Consumer Protection in the context of electronic commerce.

Principle 4: Online Privacy

[4.4] Vendors shall not disclose personal health information to affiliates or third parties for purposes other than the transactions unless specifically and expressly authorised by consumers in advance, through a clearly worded opt-in process.

[4.5] Vendors shall not, as a condition of sale, require consumers to consent to the collection, use or disclosure of personal information beyond that necessary to complete the sale.

Principle 7: Unsolicited E-mail

[7.1] Vendors shall not transmit marketing e-mail to consumers without their consent, except when vendors have an existing relationship with them. An existing relationship is not established by consumers simply visiting, browsing or searching vendors' web sites.

[7.2] Any marketing e-mail messages vendors send shall prominently display a return e-mail address and shall provide in plain language a simple procedure by which consumers can notify vendors that they do not wish to receive such messages.

The Act prohibits false or misleading representations to the public; accordingly this section focuses primarily on the application of the Act to commercial web-sites and marketing strategies using e-mail. The following table summarises the major elements of the Canadian anti-spam statutes.

*Table 12 – The major elements of the Canadian anti-spam statutes*

| Canadian anti-spam statutes | Elements |
|---|---|
| **Competition Act** | - Advertising of special products e.g. tobacco.<br>- False or misleading advertising in content of e-mail. |
| **Charter of Rights Freedoms** | - Spam is considered a form of expression. |
| **Personal Information Protection and Electronic Documents Act (PIPEDA)** | - Prohibits the collection of e-mail addresses through harvesting techniques.<br>- Requires opt-in consent.<br>- Ensures that organisations honour opt-out requests.<br>- E-mailers who establish or acquire lists of e-mail addresses must:<br>> ensure that recipients have given consent;<br>> ensure that e-mail addresses are only used for the purpose for which they are collected. |
| **The Criminal Code and the Competition Act** | - Covers fraudulent conduct.<br>- Spam that contains:<br>▪ fraudulent or false content;<br>▪ forged information in e-mail headers;<br>▪ e-mail harvesting;<br>▪ sending of "trojan" programs;<br>▪ unauthorised use of e-mail servers to send spam. |
| **Canadian Code of Practice for Consumer Protection in Electronic Commerce** | - Principle 4: Online privacy<br>- Principle 7: Unsolicited e-mail |

### 4.4.2 Effectiveness of the Canadian legislation

The legal options in Canada, as analysed above, would allow for enforcement actions against the use of deceptive headers, failure to honour opt-out requests, e-mail address harvesting, and unauthorised use of computing equipment to send spam. The Canadian Task Force will need to work with other Federal government departments and agencies to examine an effective coordinated national approach to dealing with fraudulent activities in e-mail solicitation.

On 23 September 2003 Senator Oliver rose in Parliament for the second reading of an anti-spam bill (then called Bill C-23), and several views from the Task Force were expressed (Industry Canada, 2004). Heather Black, Assistant Privacy Commissioner of Canada, noted there were many debates in the Privacy Office about whether a business e-mail address constitutes private information. Ms. Black said PIPEDA could be used to combat spam since it has jurisdiction over organisations that are engaged in consumer activity (e.g. list brokers, data miners, and spammers). Finally Ms. Black admitted that there are limits on enforcement that need to be resolved in the near future. Ray Pierce, Deputy Commissioner of Competition, Competition Bureau,

and Industry Canada, claimed that the Competition Act could apply equally to spammers, despite the fact that there is no direct mention of spam in the Act. He added that, in order to develop appropriate legislative and enforcement measures, more information is needed about the harmful effects of spam. Philippa Lawson, Executive Director, Canadian Internet Policy and Public Interest Clinic at the University of Ottawa, said that while legislation and enforcement are one piece of the anti-spam puzzle, there are many parts to the legislation and enforcement piece. There needs to be public enforcement of any anti-spam law that is enacted, she said. In addition, private parties that are affected by spam need to be able to go after the spammers. Ultimately, any anti-spam needs to be simple, to include remedies and statutory damages.

The Canadian government believes that an appropriate mix of policies and laws, consumer awareness, responsible internet industry stakeholders and technological solutions is the best and most appropriate way to deal with behaviour in the new and evolving on-line environment. The government believes that Canada has the right mix today, but will continue to monitor developments and consider changes if they are required.

## 4.5 Anti-spam law in Japan

The large volume of complaints to mobile providers resulted in the implementation of anti-spam legislation targeting messages to mobile phones (Yale Law School, 2003). Under great pressure from the telecommunication sector and the public, Japan enacted a legal solution in July 2002: the Law on Regulation of Transmission of Specified Electronic Mail (Ministry of Internal Affairs and Communications, 2003).

### 4.5.1 Key elements of the Japanese legislation

The current Japanese anti-spam legislation requires marketing e-mails to contain the text "Unsolicited Advertisement" in the subject line, and to provide the valid contact details of the sender so that e-mail recipients can opt out of receiving further communications.

*Opt-out and labelling*

In the spring of 2002, Japan adopted the opt-out regime for e-mail marketing. Every time spammers wish to send commercial e-mail communication without obtaining recipients' permission they will have to include in the e-mail message a label which will identify the message as unsolicited and commercial ("kokoku" = advertisement). In addition, spammers would have to offer a valid return address, name and postal address as well as the choice to opt out. Finally, it requires marketers to honour recipients' unsubscribe requests from further future mailings. (Ministry of Public Management, Home Affairs, Posts and Telecommunications Japan, 2003)

*Penalties*

Marketers who violate the laws face severe penalties, including fines up to $2.56 million for businesses and up to two years' imprisonment for individuals. In the bill, spam is defined as mail that is sent for vendors' advertising purposes without recipients' consent or request. E-mail senders are required to disclose their name, address and e-mail address and to inform recipients that they have the right to refuse such mail.

### 4.5.2 Effectiveness of the Japan legislation

Although Japan already has anti-spam legislation in place, the Japanese government admitted that there is a limit to how far such measures can go. Toshihiko Shibuya, Deputy Chief of Consumers Policies at the Telecommunications Ministry, stated that government measures alone cannot stop people from sending spam messages (Radio Singapore International, 2003). He also urged individual internet users to take self-protective measures against spam mail (Anti-spam Monthly Review, 2003). Enforcement of the current anti-spam law is a vital step, and the Japanese government has to consider whether the existing law should be amended and if so when.

## 4.6 The situation in New Zealand

At the time of writing this chapter, New Zealand had not yet enacted legislation to regulate spam, although various governmental departments were expressing increasing discontent with the situation (OECD Work on Spam, 2005). The government in New Zealand understood that spam infringes the privacy and harms the protection of individuals and companies, and that as a result action needs to be taken

(Office of the Privacy Commissioner, 2002). On 17 May 2004 the Government released a discussion paper with the comment that legislation may be an appropriate means of assisting in dealing with the growing problem of spam and started research to obtain feedback on the various policy issues which are raised when considering anti-spam legislation (Caslon Analytics, 2004). Australia's Spam Act 2003 has provided a useful model for New Zealand as it considers developing its own legislation to combat the global menace of UCE. Officials have undertaken research into anti-spam regimes in a number of countries to inform their work on the discussion paper. A preference for an opt-in regime is indicated in the discussion document.

## 5. Legal recommendations to combat spam

Legislation alone will not result in an immediate or dramatic reduction of spam, but it is an important element of the framework in both practice and perception. In order to implement effective legislative measures, governments should also consider an information campaign on spam issues that will target users, business communities, private-sector groups and other governmental bodies. The goals of anti-spam legislation are first to reduce and finally combat illegal spam, and second to guarantee a secure e-commerce environment for consumers and organisations. Effective legislation would give recipients of spam, both individuals and corporations, the ability to take action against offensive spammers and businesses that use deceptive techniques to forge e-mail headers, harvest e-mail addresses and send bulk mailings that people do not want.

### 5.1 Effective use of advances in IT

Lack of trust, security and harmonised national legislation, in addition to an increasing number of reported cyber-crimes, viruses, spam and fraud, have become major threats to the development of e-commerce. Providing an enabling legal framework is a fundamental need for the development of e-commerce, as it particularly affects the ability to conduct transactions on-line. Technology needs to take into account relevant legal requirements.

## 5.2 Penalties and enforcement

In order for anti-spam legislation to be effective, it must define penalties that are sufficient to act as real deterrents, and it must allow actions and enforcement to occur in a forum or court accessible to the majority of victims. Additionally, if anti-spam laws require action to be taken in the regular court systems of most countries, then the costs of simply bringing actions to court will prevent most cases, since the costs will be high. As a result, it is important for anti-spam legislation to allow victims to bring their complaints to the forum or court in an easy and cost-effective way.

## 5.3 International cooperation among the legislative bodies

The problem of spam is fundamentally an international problem, which can only be fully addressed through international cooperation and coordinated action (Gerard, 2005). Governmental bodies need to continue to participate and actively contribute to international anti-spam initiatives. Clearly one of the biggest problems with legal remedies is the number of jurisdictions involved, which leads to the conclusion that cooperation by legislators is essential. Anti-spam legislation could be considered a way of preventing spam, but most of all as a tool to punish spammers after they are identified. Arresting spammers will not stop spam, but it will contribute to the reduction of spam in the future. An example of international anti-spam cooperation is the tripartite Memorandum of Understanding on spam enforcement cooperation, an agreement between the UK, the USA and Australia to combat the problem of spam (Department of Trade and Industry, 2004a). It means that enforcement authorities in the UK, the USA and Australia will work together to investigate spammers in those countries. International solutions and strengthening capabilities will be developed to trace and convict spammers, and cross-border enforcement against spammers will take effect.

Another cooperative agreement is the London Action Plan, an international action plan that has been agreed by nineteen bodies from fifteen countries, the objective of which is to communicate and cooperate on enforcement action to tackle spam (Office of Fair Trading, 2004). The London Action Plan aims to develop international links to address spam and spam-related problems. The Action Plan encourages communication and coordination between agencies to achieve efficient and effective

enforcement, to discuss cases, legislative developments, investigative techniques, ways to address obstacles to enforcement, and consumer and business education projects, to promote ways of supporting government agencies in bringing spam cases, and to pursue their own initiatives to fight spam.

Finally, the Organisation for Economic Cooperation and Development has set up a task force to marshal the efforts of government, business and civil society in order to tackle the problems posed by spam (OECD Work on Spam, 2004b). Key objectives of the OECD will include coordinating international policy responses in the fight against spam, encouraging best practices in industry and business, promoting enhanced technical measures to combat spam, improving awareness and understanding among consumers, and facilitating cross-border law enforcement.

### 5.4 Global harmonisation in anti-spam legislation

The legal framework is a key element in the e-commerce environment that affects market participation. It is important to hold a broad public dialogue and debate with all anti-spam stakeholders before preparing e-commerce legislation, so as to ensure fairness and an equitable balance between different interests at stake (United Nations Conference on Trade and Development, 2003a). There can be no solution to the spam problem without some kind of worldwide minimum standard of legislation. Global harmonisation is a very difficult task, since the US and the EU have different opt-out/in regimes. Despite this variation, in the future we may see that the requirements for sending commercial communications around the world will be similar. For example, when the e-mail contains pornographic material, only a URL link (without indecent photographic material) should be included in the body of the message. Additionally, the subject line of the e-mail should announce that the message is pornographic.

## 6 Summary and conclusions

Spam accounts for half of all worldwide e-mail and is expected to continue to grow. It is a real and costly threat to the communications infrastructure that we increasingly rely on for social, business-related and employment purposes. The goal of this chapter was to highlight how legislative approaches can help combat spam, and specifically to

compare and contrast the legislative approaches in the USA, the UK, the EU, Australia, Canada and Japan.

As argued earlier, anti-spam legislation addresses certain problems such as intrusion into subscribers' privacy by unsolicited communications for direct marketing purposes, as well as providing clear instructions for false identities or false return addresses. However, a lot more work still needs to be done in order to tackle the problem. Legislation in isolation will not be able to eliminate spam. What is needed is a united approach, complemented by effective enforcement mechanisms, cross-border cooperation, consumer and industry education, and effective implementation of advanced technical solutions. Cooperation between anti-spam groups, legislation bodies, direct marketing groups, ISPs and anti-spam software companies adopting an integrated approach, is the most effective way to combat and eliminate spam.

# CHAPTER 7 TECHNICAL ASPECTS

The current chapter describes the technical aspects of the spam problem and evaluates anti-spam solutions. The methodology for this section is based on the creation and evaluation of a template with various technical anti-spam solutions, comparison of surveys and evaluations about ISPs' performance with spam, and use of secondary resources based on interviews with managers of ISPs and participation in IT conferences and exhibitions.

## 1. Introduction

Another approach to tackle spam is to use technical measures (software applications). Although this approach may temporarily address the problem, it is not totally effective, and also raises other issues. This chapter investigates some of the technical measures that are available, and provides an evaluation of some common applications. It finally assesses the effectiveness of technical measures adopted by ISPs and anti-spam companies, and concludes that technical means alone will not alleviate the problem.

The approach of deploying a combination of first- and second-generation measures on gateway servers is current best practice. Furthermore, despite the fact that for the last two years the performance of various technical anti-spam solutions has been improved and the rate of false positives has been reduced, the chapter suggests that a technical solution by itself is not enough. When choosing an anti-spam solution there is always an unfortunate trade-off between effectiveness in filtering out spam and the possibility of misidentifying important messages as spam, known as false positives (CipherTrust, 2005). Users may be misled in two ways – first, that a software application will resolve the problem, and secondly, that spam is a fact of information society life and their own responsibility to resolve. That is an unfair burden on users. Cooperation between anti-spam developers, legislation, marketing and ISP associations is the most effective way to combat and manage spam.

## 2. Evaluation of anti-spam solutions

One of the first steps in tackling the problem of spam is to decide what type of protection is needed. From a practical and technical perspective, spammers have only

one point of entry: whereas viruses can penetrate a network from multiple points (web access, web-mail, floppy disks, etc), spam enters from only one place, the e-mail application. Technical measures (software applications) temporarily address the problem, but they also raise other issues.

## 2.1 First-generation anti-spam solutions

Some solutions use lists of known spammers, discarding messages originating from those addresses or domains. One such offering is the MAPS Realtime Blackhole List (RBL), a free service run by the Mail Abuse Prevention System, a non-profit organisation dedicated to making the internet as spam-free as possible. RBL is a global clearing house of information about systems which originate spam and systems that provide support services to spammers. The idea behind RBL is that a subscriber's e-mail server will consult the MAPS database as each piece of mail is received, and check the sender against the blackhole list (Harris, 2003). If the message comes from a site on the list, it can be discarded, or at least marked as probable spam, before it hits the user's mailbox.

Use of a blocking list can give rise to only one response – to block reception. This technique cannot differentiate between individual e-mails: all e-mail from a black-listed source will be blocked. However, for some types of spam, e.g. known pornographic spammers, blocking is typically the best approach. In general, though, using the black-list approach to control spam is not effective since the originating address of a message can be spoofed much more easily than the address of a web page. Spammers usually forge their identity and can make e-mails look as though they originate from innocuous addresses, or they can continually change the addresses from which their messages seem to originate. There are cases where free web-mail services (hotmail, yahoo) are abused by spammers. Using the RBL approach care should be taken concerning which domain name is included in the blackhole list in order not to block legitimate e-mail communication from domains like hotmail or yahoo.

The first-generation anti-spam solution also includes recipients' filtering software and keyword filters. The limitation of using this approach is that keyword filters should be updated frequently and customised according to the needs of the corporation.

## 2.2 Second-generation anti-spam solutions

Second-generation solutions include a signature-based approach similar to an anti-virus scheme. Vendors use "honeypots" to attract spam. An example of a honeypot is the Probe Network concept introduced by Brightmail. This system consists of strategically placed, dedicated e-mail accounts, which serve as an early warning system for the detection of spam and viruses. The system is in continuous operation. With a statistical reach of over 150 million mailboxes, the Probe Network includes special probe accounts disguised as regular e-mail addresses, allowing Brightmail to catch and analyse spam attacks in their early stages. The Probe Network delivers the latest spam attacks to anti-spam technicians at the Brightmail Logistics and Operations Centre (BLOC), where technicians evaluate them and create customised rules to disable each attack. By the time spam is poised to invade a user's inbox, the Probe Network has discovered it, the BLOC has prepared rules to block it, and the Brightmail server apprehends it. The spam is blocked before it can reach the inbox. The diagram below (Figure 14) describes the concept of the Probe Network.

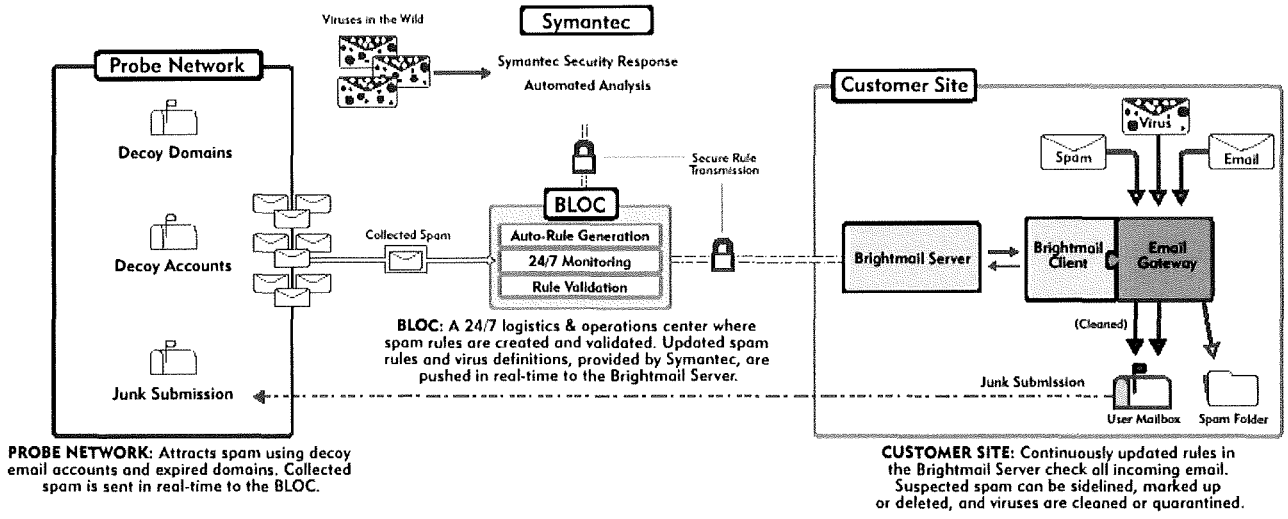



*Figure 14 – Brightmail: the Probe Network concept*

Distinguishing spam from legitimate e-mails is not an easy exercise. Content filtering appears to offer a solution, but an assessment of what is or is not legitimate has to be made. This naturally raises the questions of who makes the decision about what words are offensive, and of third parties reading or scanning, your e-mail (inbound as well as outbound). There are several cases where ISPs have incorrectly blocked legitimate

personal communication as unwanted e-mail. Legitimate messages were wrongly tagged as junk mail, half went to junk mail folders and half were never delivered.

The following paragraphs evaluate some of the technical anti-spam solutions. The diagram below (Figure 15) gives the basic infrastructure arrangements involved.

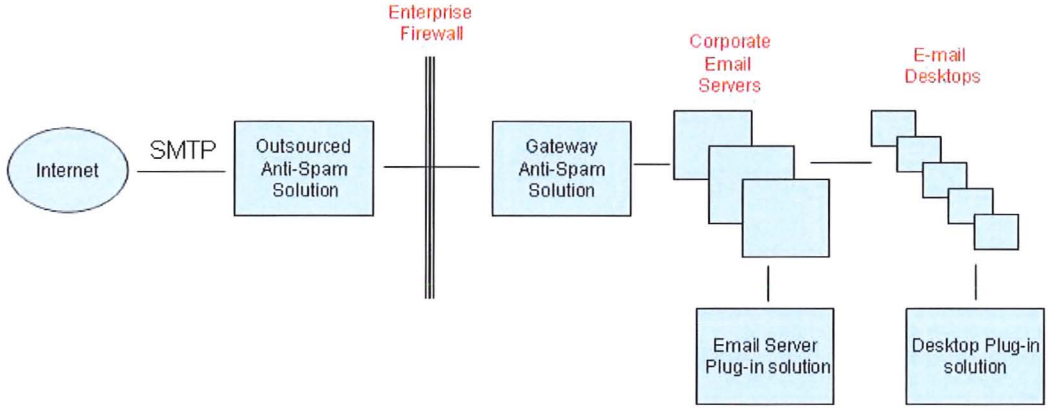



***Figure 15 – Infrastructure of path used by in/out-bound spam***

### 2.2.1 E-mail server-based anti-spam solutions

Blocking spam at this point in the network saves a significant amount of employee productivity. However, server plug-ins tend to degrade the performance and uptime of mail servers. Server-based solutions are cost-effective for smaller organisations that have only a single e-mail server for the entire organisation (less than about five hundred accounts). However, it is not a cost-effective approach for organisations with multiple e-mail servers.

### 2.2.2 Client-side anti-spam solutions

Client-side anti-spam solutions work reasonably well and allow end-users to customise blocking capabilities to fulfill their individual needs. They are however primarily consumer-focused, and require end-users to spend time managing an additional application: that has a productivity cost as well as consuming corporation bandwidth and storage capacity. Using a client-side solution means that enterprise-wide policies cannot be enforced. In general, client-side anti-spam solutions are most appropriate for small businesses and individuals.

### 2.2.3 Gateway-based anti-spam solutions

This type of anti-spam protection sits between an organisation's firewall and its corporate e-mail servers, and takes one of two forms. The first form, the e-mail relay plug-in, is an application integrated with the SMTP relay that processes inbound and outbound e-mail. It adds a spam-filtering step to in-bound message processing. The second form is the e-mail firewall, a stand-alone application that provides a broad set of e-mail filtering functions. It eliminates most spam before it reaches the end-user, and provides good network resource benefits since spam is blocked before it enters the corporate network. This method eliminates the need to manage individual spam applications installed on every e-mail server or desktop, and benefits from access to the SMTP protocol-level and network-level information available at the gateway: that leads to more effective spam-blocking. One of the negative characteristics of this solution is that it requires more time and resources, including software, network resources and IT administration. A gateway-based solution is the best approach for larger companies with more than about five hundred e-mail accounts.

### 2.2.4 Outsourced anti-spam solutions

Outsourced anti-spam solutions (Messagelabs, FrontBridge Technologies, Postini) redirect an organisation's in-bound e-mail stream to a third party for inspection. Giving to a third party the responsibility to decide what e-mail is spam and what is legitimate is often a difficult decision for larger organisations with increased security requirements. The outsourced anti-spam solution involves some risk in terms of the unknown reliability of the third party. Usually outsourced solutions are cost-effective and more suitable for SME organisations that lack expertise or resources to manage the problem of spam internally. It improves the end-user's productivity and eliminates network costs in relation to spam because it filters spam before it enters the corporate network. The two major disadvantages are that it can be a very expensive solution and also that it reduces the organisation's e-mail control since a third party is responsible for the inspection.

## 2.3 Bayesian filtering

The concept of using automated statistics-based categorisation to identify spam is not at all recent, but the idea became better known with the publication by Paul Graham of "A plan for spam" in August 2002. Graham used what he called Bayesian filtering to identify spam, and trained a spam filter to give individual words a score based on the frequency of their occurrence in spam and non-spam e-mail. He then tried to determine whether a given e-mail was spam by looking at the scores of the words within it. Graham claimed some very impressive results: 99.5 per cent detection of spam, with no false positives. This method works best when each individual user has their own probability dictionary – which tends to be considered impractical by commercial anti-spam vendors, mainly because a good dictionary will be around 4 to 10MB per user.

Bayesian filtering algorithms (NetworkWorldFusion, 2003) calculate the probability of a message being of a pre-determined type based on its contents. "Bayesian filtering is based on the principle that most events are dependent and that the probability of an event occurring in the future can be inferred from the previous occurrences of that event" (GFI, 2004).

Here is an example of how statistical (Bayesian) filtering works (Graham, 2002): There is one corpus of spam and one of legitimate e-mail and each one of those contains about five thousand messages. The first step is to scan the entire text of each message in each corpus, including headers, embedded html or JavaScript. We consider alphanumeric characters, dashes, apostrophes and dollar signs to be parts of tokens, and everything else to be token separators. We also ignore tokens that are all digits, and html comments, not even considering them as token separators. Then we count the number of times each token occurs in each corpus and at the end of this stage we end up with two large hash tables, one for each corpus, mapping tokens to number of occurrences. Next we create a third hash table, this time mapping each token to the probability that an e-mail containing it is spam. Because the Bayesian approach measures probabilities, it takes into consideration all the evidence in an e-mail, both good and bad. Words that occur rarely in spam, like "ultimately" or "apparently", contribute as much to decrease the probability as bad words like "unsubscribe" or "opt-in" do to increase it. This makes it possible for a legitimate e-

mail that includes the word "sex" not to get tagged as spam: the probabilities are calculated individually for each user. So if spammers start using "V1@grA" instead of "viagra" to trick simple-minded spam filters, Bayesian filters automatically notice that "V1@grA" is more likely to indicate that an e-mail is spam than "viagra", and will determine the difference in likelihood.

Bayesian filters, after training, can be more effective than other types of anti-spam filters. Without sufficient training, however, the performance of Bayesian filters can be poor in comparison other technical anti-spam methods. Based upon the results of Infoworld.com (Harbaugh, 2004), PC Advisor (PC Advisor, 2004), and Accudata Systems (Accudata Systems, 2004), SpamProbe and Bayesian Mail Filter have usable recall percentages and acceptable precision. Unlike simple content-based filters, Bayesian filtering learns from both spam and legitimate mail (or any other assigned categories) (Overton, 2004).

Anti-spam filters such as SpamAssassin assign a spam score to e-mail. The Bayesian approach assigns a probability. SpamAssassin lets through more spam than Bayesian filters, but has better results in false positives. Quick Spam Filter performs poorly when compared with other Bayesian filters. It is recommended not to delete spam automatically but to file suspected messages in case there are false positives. If an e-mail is tagged as spam by an anti-spam filter, but that judgment is not correct, then the message should not be deleted but manually moved to the junk folder. In this way a collection of spam and non-spam messages will be built up which will be useful for training the anti-spam software.

## 3. Summary and conclusions

Bayesian filters are not very effective if they are not trained; and that can only be achieved by having a collection of past e-mails (both spam and legitimate). If the anti-spam filter supports white lists, then it is useful in order to enable legitimate e-mail addresses to be included. Additionally the junk folder needs to be scanned often in order to check for e-mails that are legitimate. Training will be based on the collection of classified spam and legitimate e-mail messages, or on the messages classified as false positives or false negatives so as to correct the mistakes (Robinson, 2003). Once spam and legitimate e-mail messages are correctly classified, Bayesian filters can be

used effectively to tackle spam. The bigger the classified list is the better Bayesian filters will work since training is the keyword when using a learning filter. Formula-based filters, without significant end-user intervention, have high false positive rates. The need for human analysis when filtering spam is high, since this is the only way to catch most spam without generating high percentages of false positives (Zixcorp, 2003).

# CHAPTER 8 CORPORATE E-MAIL POLICIES

This chapter explores the risks involved with employee e-mail use, discusses the framework that will govern an effective e-mail policy and provides organisations with a comprehensive view of e-mail security through the development of corporate e-mail policies. The development of a corporate e-mail policy is a vital element for an organisation in order to tackle the problem of spam. It provides information for any business that is looking to put appropriate security controls in place to protect its information. The current chapter provides solutions for a spam-free corporate e-mail system and concludes that employees need education and training to improve their behaviour towards spam.

## 1. Introduction

Given the large volume of e-mail use, it is no surprise that e-mail has become the most common means of business communication. It is important for organisations to understand the potential for making the most of their information systems as well as the opportunities that the use of the internet and e-mail offer. Though e-mail offers unique benefits and challenges, its convenience and efficiency have been dramatically reduced by the extremely rapid growth of UCE (Law Society, 2004).

Regardless of industry type, company size, status as a for-profit or not-for-profit entity, the accidental misuse and intentional abuse of e-mail by employees, as well as the challenge of controlling electronic communications as they flow into and out of an organisation, is becoming increasingly critical (Flynn, 2003). Many organisations are trying to reduce these risks by controlling employee use of e-mail through the implementation of employee Acceptable Use Policies (AUPs) and enforcing these by implementing technical solutions.

## 2. E-mail threats

The main problem an employer risks facing when employees use the internet, whether under European or American Law, is liability for an offence committed by an employee in the exercise of his or her functions and particularly in the workplace (Rosenoer, 1996). Generally, employers are liable for those who work under their orders and can only evade that liability in certain specific cases stipulated by national

legal systems. Thus in certain cases an employer can escape liability by proving that the act in question constitutes gross negligence (sabotage, hijacking of files), or a serious offence (unauthorised access to protected files), or that it has been specifically forbidden in the employment contract (for example, by means of an Acceptable Use Policy). Although the employer is liable for employees' activities, the latter obviously remain responsible for their own offences. Hence the victim of a forgery can often take action against the employee or the employer, or both (Hance, 1997).

Despite the obvious benefits of using e-mail in the working environment, the organisation should consider possible problems. Among the most common e-risks of using e-mail are security breaches, malicious hacker attacks, lost productivity, wasted computer resources and public embarrassment (Flynn, 2000). E-mail places employers at risk of litigation when employees use company e-mail inappropriately; as a result, their actions can harm the entire organisation (BorderWare Technologies Inc, 2004). Inappropriate use may include minor cases, such as employees wasting time surfing the internet or sending personal e-mails, or slowing down the system with large attachments and copying large numbers of people in on e-mails unnecessarily (Business Link, 2005). Based on a survey by IDC, the time spent as a result of damage caused by viruses coming in via spam is the biggest organisational cost (Figure 16). Similarly, they believe that worms and viruses are increasingly using spam techniques (Burke, 2004).

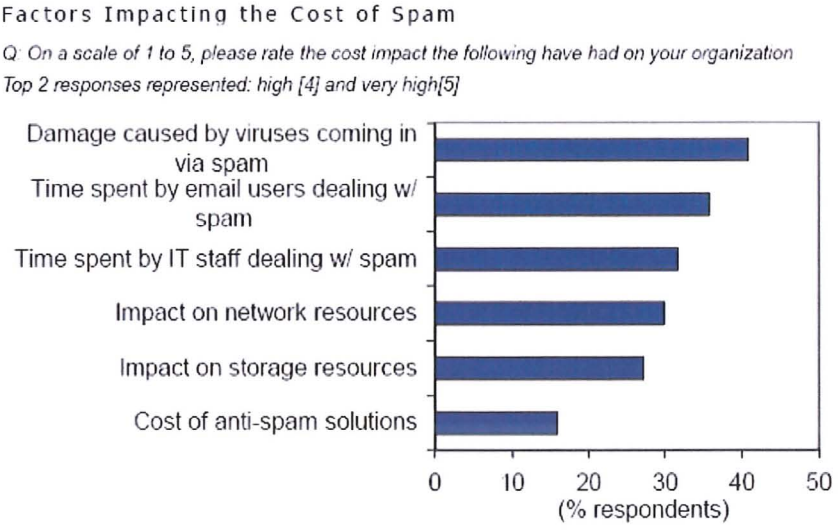



***Figure 16 – IDC's spam study, 2003***

### 2.1 Breach of confidentiality

Other more serious risks for corporate security include breach of confidentiality. There is always the risk that an employee may accidentally or intentionally disclose confidential information in an e-mail. Such disclosure could take the form of forwarding an e-mail to the wrong recipients or misaddressing an e-mail; it could also happen intentionally as industrial espionage. Either way, the result will harm the organisation. The law that regulates confidentiality is continuously developing. In the EU the Working Party, an independent EU Advisory Body on Data Protection and Privacy, was established by Article 29 of Directive 95/46/EC. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC. It states that no possible surveillance is allowed unless it is necessary for legitimate purposes, and provides clear and comprehensive information about monitoring employees in the workplace. The Data Protection Act 1998, which came into full force in October 2001, regulates the use of personal information such as customers' names and addresses or even health records. The Act is based on a set of principles related to the lawful handling of data, and it requires organisations to inform individuals about how their data will be used and makes sure that their consent will be obtained. The Act imposes strict legal requirements on everyone processing personal data. It is important to note that organisations processing personal data are required to have "appropriate organisational and technological measures" in place to safeguard the data. Failure to comply with the Act may result in penalties ranging from fines up to criminal sanctions.

### 2.2 Defamation and obscenity

One of the increasing problems faced by any business is the ease with which it can be defamed and/or accidentally face an action for defamation. Just like any form of speech or communication, a statement published on-line which "would tend to lower the plaintiff in the estimation of right-thinking members of society generally or cause him to be shunned or avoided or tend to expose him to hatred contempt or ridicule" may be actionable as defamation. Employers may be liable for the actions of their employees and are exposed to greater risk as the internet provides a medium in which anyone can easily publish a message which will reach a large number of people virtually instantly, without having to go through an intermediary like a newspaper or

book publisher who would be in a position to check it. The defamatory statement must be "published" by communicating it to at least one person other than the person defamed. An e-mail containing a statement defamatory to the addressee cannot normally be the subject of an action unless it can be proved that a third party did in fact read the e-mail and the defendant intended, or should have foreseen, that the e-mail would or could be read by someone other than the intended recipient (York, 2002).

While defamation is more serious than simple abuse, it is recommended that companies need to take seriously all types of illegal activities. A key risk associated with defamation is that each repetition of the statement may be a new defamation. For example, if an employee (company X) sent another employee of a different company (company Z) a defamatory e-mail; and as a result of the statement company Z suffered loss, then company Z could sue the sender and his employer. Additionally, if the e-mail recipient forwarded the message to another employee within company Z then that is a new defamation, and company Z may also be able to sue the forwarder.

Obscenity can also be a serious problem for organisations. If for example an employer receives an e-mail from a friend at his corporate e-mail account during his break, and enclosed within the message is a pornographic image, which he then uses as wallpaper for his desktop, there is always the possibility of the image being seen by another employee, who may be offended. The consequences could be serious for the company, since an employment tribunal may find that the organisation has not taken the necessary steps to prevent an atmosphere of obscenity in its offices. Continuing the example, the recipient of the obscene e-mail forwards the attachment to a friend in another organisation, who in turn forwards it to several other recipients. All the above recipients can easily spot, after reading the list of people which are involved in the forwarding list, that one of the first senders is an employee of the organisation that was mentioned above, something of course that will damage the reputation of the business even further.

Standards for the determination of obscenity also vary widely. In the UK, for example, the definition of obscenity is based on the potential effects of the material on its readers or viewers. In s 1(1) of the Obscene Publications Act 1959 obscenity is defined as follows: "An article shall be deemed to be obscene if its effect or the effect

of any one of its terms is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regards to all relevant circumstances, to read, see or hear the matter contained or embodied in it" (Reed, 2003).

### 2.3 Wasted time and resources

Junk e-mail not only costs corporations dearly in precious network resources and employee productivity, but may also carry with it serious legal liability, as well as network security risks. The cumulative costs add up quickly when employees spend a few minutes a day dealing with and disposing of spam. Organisations need to examine what percentage of their labour costs is lost because employees are sifting through junk e-mail, not to mention the diversion of attention of data centre and MIS staff. There are other productivity drains as well: on a legal front, there have been many instances of lawsuits as a result of pornographic and other messages circulated via e-mail in the workplace. Spam blocks corporate mailboxes, making it difficult for users to find important messages (Kille, 2003). It is also reported (Gradwell, 2003) that instances of hidden e-mail threats such as viruses (Mailwasher, 2001b) that are included in spam e-mail messages are on the increase. Another important issue is the efficiency of corporate information systems when large quantities of huge messages are transmitted and stored. Data retention is a serious issue for organisations today since several systems have collapsed due to the sheer bulk of spam.

### 2.4 Contractual liability – liability for defective products

Many contracts are now completed through the internet and in particular with the use of electronic mail. The terms of the contracts are usually included somewhere in the exchange of mails. Defective products are a good example of an area where an e-merchant could face potential liability, and are a useful starting-point from which to discuss the basic principles of liability generally. Conducting business using e-mail runs the danger that an employee may enter into a contract by e-mail without authorisation and commit the business to an obligation that it cannot fulfil. In that case, the business may face an action for breach of contact with serious further consequences in terms of both finances and reputation.

Another risk associated with e-mail contracts concerns misrepresentation of a product or service. The employee might be over-enthusiastic about the benefits of the product

or service and mislead the customer to buy something that is misrepresented. The business may face an action for misrepresentation when the customer discovers the truth about the capabilities of the product. The customer may use the e-mail communication with the seller as proof to show that the product or service as purchased does not match the product description received from the seller. Where there is a direct contractual relationship, e-merchants can be liable to their customers for supplying defective products because it may be a breach of an express term of the contract (e.g. to deliver goods of a specified description and quality) or a breach of an implied term of the contract (e.g. in the UK, the Sale of Goods Act 1979 implies terms in the contract that the goods will correspond to their description).

### 2.5 Intellectual property issues

Copyright arises automatically when a right, which is usually owned, either by the producers of the material or their employers, is created and does not have to be registered. If the employees of a company download, copy, forward or alter copyrighted material on-line they are running the danger of infringing these rights, and in that case the business will face an action for infringement. Employees often open e-mail attachments that contain malicious program code such as viruses without being aware of the negative consequences. Unfortunately, some are hidden in useful applications. The user who downloads the file is not aware that, in addition to the useful code, the file contains destructive code, which erupts either immediately or some time after the download. Such a virus is called a Trojan horse.

Aside from the risk of virus infection, many of the software programs available on-line are copyright-protected, and licenses are required before software can be lawfully used. Possession of infringing copies of software applications in an organisation can lead to corporate liability, and directors can face the threat of personal liability. The Copyright, Designs and Patents Act 1988 gives the same protection to digital and electronic publications as it does to printed books and other forms of publication. Many websites carry warnings that the information given is copyright and should not be downloaded without agreement from the copyright holder. Similarly copyright exists over mp3 music files from the internet, which should not be downloaded without a license. The following table (Table 12) summarises the corporate e-mail threats and e-policy initiatives that can be implemented.

*Table 13 – Corporate e-mail threats and e-policy initiatives*

| Corporate e-mail threats | E-policy initiatives |
|---|---|
| **Breach of confidentiality** | - Make sure an e-mail policy is in place that stating: *"Deliberate releasing of confidential information is a disciplinary offence".*<br>- Develop carefully worded e-mail disclaimers with reference to disclosure of confidential material. It is recommended that the disclaimer dealing with confidentiality should be at the top of the e-mail so that recipients have notice of it before reading the e-mail. Such a disclaimer could read: *"Information in this message is confidential. If you are not the intended recipient, please notify the sender, and delete the message from your system immediately".* |
| **Defamation and obscenity** | - Education together with an effective e-mail policy can be the answer to avoid liability.<br>- It is very important that employees fully understand the terms of the e-mail policy, in particular what they are not allowed to include in business e-mail communications and what they can or cannot view or download from the internet.<br>- Monitoring in the work-place. |
| **Wasted time and resources** | Through the corporate e-mail policy an organisation should determine:<br>- which employees will have internet and/or e-mail access;<br>- whether non-business activities, using corporate e-mail address, are allowed;<br>- if non-business activities are allowed, what level of personal use is permitted.<br>Consultation with employees is a good practice to communicate the e-mail policy across the departments of the organisation. |
| **Contractual liability; liability for defective products** | - Corporate e-mail policy should make it clear to employees how much authority they have to alter business contracts.<br>- Inclusion of an appropriate disclaimer in the e-mail message can help minimise risks in this area. For example: *"The company does not enter into contracts with a value more than £10,000 without a signed hard copy".* |
| **Intellectual property issues** | - An e-mail and internet policy should make clear to employees that they should not infringe copyright and educate them about copyright legislation.<br>- Employees could be banned from copying material online without permission. |

## 3. Spam and corporate e-mail policy

The issue of security for computer systems and company information is a major concern for employers who take various preventative measures to deter and combat inappropriate use of e-mail, and in general of the internet, by employees. Although many businesses are not able to spend a large amount of money developing and maintaining a web site, even the smallest business can afford to use e-mail. To avoid inappropriate e-mail usage, it is important to clarify what is permitted by the organisation and what is not, by introducing an e-mail policy (e-Policy Institute, 2004). Since e-mail policies usually describe what employees are not allowed to do (i.e. access adult content using corporate infrastructure), prevention would appear to be the primary purpose of a corporate e-mail policy (Forsite Group, 2004). However,

the major objective of a corporate e-mail policy is to protect the organisation from various internal or external threats and to act as the element that binds all aspects of information security management (Department of Trade and Industry, 2004b-d).

Enterprises play a double role in the spam case. At first they do not want to receive from third parties any spam, but most of them wish to use e-mail as a marketing tool. There's no magic formula for creating an effective e-mail policy. The objective is to cover as many situations as possible, even without awareness of what some of them will be. Since all organisations are different, it is expected that e-mail policies will vary as well. If the organisation wishes to handle spam, it has to focus first on the receiver: as a result, one of the first steps that organisations should take, prior to implementing any type of software or technology solution, is the development of an e-mail policy that clearly details how spam is handled. While most organisations have developed e-mail policies, many lack the specific detail required to inform employees how to deal with inappropriate e-mail (Haftke, 2000).

According to the 2003 research published by ClearSwift, a company responsible for managing and securing electronic communications, despite the serious concerns over reduced productivity levels over one-third (37 per cent) of UK organisations do not have a policy in place to fight spam (ClearSwift, 2003). The survey reveals that, while action is being taken at government and industry levels to raise awareness of the implications of spam for the wider economy, businesses are failing to establish e-policies, educate employees and implement advanced counter-spam solutions. The following table (Table 14) summarises the e-mail threats and their negative effect on organisations and identifies the elements that need to be added in a corporate e-mail policy in order for the problems to be tackled.

*Table 14 – Identifying e-mail threats in the corporate e-mail policy*

| E-mail threats/spam | Negative effects | References in the corporate e-mail policy |
|---|---|---|
| **Spam** | Spam is a major concern for organisations:<br>- illegal product information;<br>- loss of productivity;<br>- reduction of network bandwidth;<br>- increased risk of virus infection and other malicious code;<br>- increased risk of liability and legal action. | - Be aware of what you sign up online: make sure you read the privacy policies of the site involved, since some may sell your e-mail address.<br>- Be aware of check boxes in sign-up forms that, when left unchecked, allow the company to share your information with other firms.<br>- Forwarding: continuous forwards can result in anyone being able to harvest several e-mail addresses from just one of these bulky e-mails.<br>- Do not reply to spam and do not respond to messages that offer an unsubscribe option.<br>- Delete, block and report junk e-mail messages.<br>- Do not purchase any products through spam. |
| **Identity theft** | - The use of information about an organisation (or an individual) to infer its identity. Later efforts to obtain goods or services using that identity.<br>- E-mail spoofing: Fraudsters forge e-mail headers to elicit information as part of a seemingly legitimate transaction. | - Check the e-mail headers to identify who is the real sender of the e-mail.<br>- Do not give personal information in an e-mail.<br>- Do not share your primary e-mail address with people you know.<br>- Avoid listing your e-mail address in large internet directories. |
| **Phishing** | - Sending false e-mail messages to a wide audience. Phishing e-mails are designed to look as if they come from a legitimate organisation asking recipients to confirm their account details and damage the reputation of the organisation.<br>- Fraudsters use spam-lists in the hope that some people will reply. | - Do not respond to e-mails asking for security details or financial information of the organisation.<br>- If you receive such an e-mail delete it and do not open any attachments.<br>- Visit banks' websites by typing the URL into the address bar.<br>- Keep a regular check on your accounts.<br>- Check the website you are visiting is secure. Also look for a lock icon on the browser's status bar.<br>- Check the web address in the address bar.<br>- Be cautious with e-mails and personal data.<br>- Always report suspicious activity. |
| **Frauds, scam and misuse** | Inappropriate use:<br>- reveal confidential corporate information and sending of sensitive data to spammers (private use or disclosure of customer lists, price lists etc);<br>- employees replying to spam e-mail messages or even shopping online from spammer's insecure web-sites during work hours;<br>- viewing, downloading or distributing pornographic material received from spammers. | Under no circumstances should the organisation's e-mail system be used to send, receive, browse, download or store material which may be illegal, offensive or cause embarrassment to others.<br>- This includes the use of the corporate systems for: viewing, sending, receiving, downloading or distributing material which is pornographic, racially or sexually offensive.<br>- Think twice before opening attachments or clicking links in e-mail or instant messages, even if you know the sender. If you cannot confirm with the sender that an attachment or link is safe, delete the message.<br>- Do not forward chain e-mail messages. |

## 4. The structure of an e-mail policy

In general, policies are usually based on existing published standards which provide specifications for developing an information security management system (ISMS). There are several sources that have had considerable impact on developing policies, such as the Cadbury (Cadbury Report, 1992) and Turnbull (Institute of Chartered

Accountants in England and Wales: 2005) reports. The British Standards Institute (BSI), has developed the BS 7799 (BS 7799-2, 2002) and the ISO/IEC 17799 (ISO/IEC 17799, 2000) a useful set of guidelines, which provide advice on implementation and auditing aspects. The BS 7799 standard provides specifications about designing, implementing and updating an information security management system and the ISO/IEC 17799 code of practice is designed to identify the range of controls needed when information systems are in use.

A corporate policy establishes the boundaries and uses that may be made of organisational equipment. Policy development may be achieved by use of a working party, with representatives of IT, personnel/human resources, staff and other directly interested parties such as security advisers. This section analyses the format for structuring an e-mail policy.

***General title - version number***

The title indicates the main idea of the policy. In this case a possible title could be 'Corporate e-mail policy for 'x' Corporation – Guidelines for e-mail use'. The version number is important to ensure that the most updated policy is applied.

***Introduction - executive summary - purpose***

This is usually a single page that allows the reader quickly to understand the purpose and the scope of the e-mail policy. The purpose is to ensure that employees of the organisation and its subsidiaries understand the way in which e-mail should be used in the organisation. It aims to ensure that e-mail is used effectively for its intended purpose without infringing legal requirements or creating unnecessary business risk (SurfControl, 2003).

***Definitions***

Since an e-mail policy needs to be clear and understandable, this section is important because various technical terms will be used and may be unknown by most employees. It is important to remember that the definitions will be used in the context of the policy and the meaning should not change.

***Scope***

This section needs to define the people to whom the e-mail policy applies and in what circumstances. For example the policy may only apply to full-time employees or only to managers.

***Roles, responsibilities and objectives***

The roles and responsibilities are related to the *scope* section. This part describes what level of responsibility will be undertaken by a staff member or a department within the organisation. For example the Information Security Manager is responsible for developing and updating other corporate documents to ensure that e-mail policy is supported by appropriate and relevant documentation and has been communicated among the departments of the organisation. A set of objectives will enable the Information Security Manager to establish the principles by which he wishes the e-mail policy to operate.

***Policy***

This is the main content of the document, informing employees about the acceptable use of e-mail within the organisation.

The Department of Trade and Industry in UK suggests the following steps for developing an e-mail policy (Department of Trade and Industry, 2004b-d).

- Conduct research in relation to the policy content.
- Develop a draft version of the policy.
- Obtain senior management approval.
- Circulate the policy to all staff.

# 5. Inside the corporate e-mail policy

## 5.1 General guidelines

Initially a centrally managed policy must ensure that the individual requirements of departments, teams and users are successfully met (Group Technologies Corporation, 2005). The corporate culture will determine how far an e-mail policy can go in strictly managing e-mail use. An e-mail policy that is well written and effectively communicated to all employees is one of the best ways for employers to protect themselves from the risks associated with the inappropriate use of e-mail and internet systems. It should state what is considered appropriate and inappropriate content for e-mail and how employees should handle unsolicited e-mail, especially if the e-mail contains offensive, obscene or indecent material, such as pornography, racist or sexist material, violent images, incitement to criminal behaviour, etc.

### 5.2 Clarity of e-mail policy, corporate education and awareness

Companies' e-mail use policies must be crystal clear, relevant, accessible and understandable to all intended users, and define the types of communication which are allowed in the organisation (Bolles, 2003). The success of an e-mail policy depends on effective communication with staff, making them aware of the negative effects of spam (Computer Associates Corporation, 2004). Any initiative for developing an e-mail policy should be accompanied by a parallel education and awareness initiative. This depends on several different factors such as the level of perceived risk, available budget, available technical infrastructure, geographic spread of the organisation and the diversity of the corporate culture (Department of Trade and Industry, 2004b-d). Employees must be properly educated about the e-policy to ensure that they fully understand it and its importance as a corporate asset. Education should require written acknowledgement of the policy and should involve frequent e-policy reinforcement.

### 5.3 Establishment of netiquette policies for e-mail senders and receivers, both managers and staff

a) Instruct users never to reply to spam e-mail messages or to "unsubscribe" options. Often the reply accomplishes just the opposite: It confirms the validity of the recipient's e-mail address and encourages the spammer to send more e-mail or to forward the e-mail address to other spammers. Replying to spam also can be a waste of time, as senders sometimes use a disposal address for sending their spam. Notify employees not to forward junk e-mail messages to other co-workers (Department of Trade and Industry, 2004b-d).

b) Often employees copy everyone on every e-mail they send, creating dozens of long message threads that qualify in some recipients' minds as "unsolicited bulk e-mail". It is important to send e-mail messages only to readers with a legitimate need for them as well as to mail to a group list only when it is appropriate for everyone on the list to receive the message.

c) Employees should not provide their e-mail addresses to unfamiliar web sites.

d) Subscribe to real-time blackhole list services that block delivery of e-mails from known spammers.

e) Subscribe to a Signature Database List and update regularly, which will prevent the delivery of known spam and other digital junk.

f) Install content filtering tools that scan and block e-mail messages which include suspect subject lines or text like "Get rich quick".

g) Before sending an attachment, the sender can ask if the reader would prefer to receive the information as an attachment or as part of the message itself.

### 5.4 Personal use

In addition, the e-mail policy needs to detail how employees can use e-mail for personal use: for instance it may determine whether or not employees can sign up for on-line newsletters, in which case the policy needs to state the conditions for selecting a newsletter and for ensuring that is business-related and meets the organisation's guidelines. Policies that attempt to forbid all personal use of company e-mail turn the organisation into a strict and boring environment and the IT department into internet police. Most policies need to establish a balance between business and personal use, while encouraging staff to develop effective computer skills (Acas Organisation, 2004).

### 5.5 Evidence and data retrieval

An effective e-mail policy is responsible for addressing the issue of e-mail management. The failure to store, monitor and retrieve e-mails on a corporate network can lead to costly legal wrangles and damaged business relationships. Problems may be caused by deleting e-mails that might be needed later for legal purposes. When an e-mail policy is combined with reporting, it becomes a very powerful tool that can track violations in the policies. The use of reporting gives the company evidence to take action against violators.

### 5.6 Disclaimer statement for outgoing e-mails

It is advisable for a statement relating to e-mail transmission to be included in every outgoing e-mail. Such a statement could read as follows.

Although [company name] has taken steps to ensure that this e-mail and attachments are free from any virus, we advise that, in keeping with good computing practice, the recipient should run a check to ensure they are actually virus-free. If you are not the intended recipient of this e-mail (and any attachment), please inform the sender by return e-mail and destroy all copies.

Communication by internet e-mail is not secure, as messages can be intercepted and read by someone else. Therefore we strongly advise you not to e-mail any information which if disclosed to unrelated third parties would be likely to cause you distress. If you have an enquiry of this nature please provide a postal address to allow us to communicate with you in a more secure way. If you want us to respond by e-mail you must realise that there can be no guarantee of privacy.

### 5.7 E-mail confidentiality

Electronic mail is not a secure medium of communication even when encryption or other security methods are adopted. It may still be possible for persons other than the sender or the intended recipient to intercept and gain access to the message. It is therefore important for organisations to consider carefully, before an e-mail message is sent, whether e-mail is the most appropriate way to communicate with customers and business partners. According to the European anti-spam legislation, e-mail must not be sent to customers/clients without their prior express consent (authority). In certain circumstances, the contents of any electronic message may contain material that is confidential to a third party. In these cases, it may be necessary to seek permission from the third party before the message is sent.

### 5.8 Level of monitoring

The decision whether to monitor systems and information should be part of the initial development of the policy. All organisations are likely to install anti-virus software to protect their systems, but there are many other forms of software available which can be used for automatic blocking and monitoring of the flow and content of communications (Bagnall, 2000). It may be possible to exclude private e-mails (where these are allowed) from being monitored by the organisation's monitoring system. If private e-mails can be monitored then the consent of staff should be sought. It is permitted, however, to monitor e-mail solely for the purpose of determining whether it is a business communication or a personal one. Firms should review the following legislation when establishing e-mail monitoring, storage policies and practices.

a) The Regulation of Investigatory Powers Act 2000 (RIPA) creates several offences and a statutory tort of interception of a communication in the course of

its transmission without lawful authority. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 sets out various circumstances in which monitoring and recording of e-mail for business-related purposes is deemed to have lawful authority.

b) The Data Protection Act Part 3 of the Information Commissioner's Employment Practices sets out guidelines for organisations to consider when monitoring or recording e-mails in the workplace.

c) The Human Rights Act 1998 is also relevant in monitoring activities in the workplace. In particular, Article 8 of the European Convention on Human Rights provides that "everyone has the right to respect for his private and family life, his home and his correspondence". Though the provision is directly enforceable against public sector employers, and businesses are not public authorities, all courts must now interpret existing legislation in relation to the Human Rights Act of 1998. Therefore the Human Rights Act 1998 does not apply to them directly, but courts are increasingly taking human rights cases into account in their decisions. According to the provision, the right to privacy extends to the workplace and suggests that employees may have reasonable expectation of privacy in the workplace. Employers are recommended to allow workers to make personal communications that are not subject to monitoring.

### 5.9 Informing employees and recipients about e-mail monitoring

Employees should of course be made aware via the organisation's e-mail/internet policy what software monitoring systems are installed, how they work and why they are necessary for the business (Law Society, 2004). Recipients of e-mails need to know whether monitoring is taking place or may take place. A standard footnote can be added automatically to external e-mails, indicating that the organisation may monitor communications for business purposes. Such a footnote may also contain a disclaimer and statement that the communication is for the intended recipient only. Organisations should note the Information Commissioner's Employment Practices Data Protection Code Part 3, Monitoring at Work, makes the following recommendation.

> If monitoring is to be used to enforce the organisation's rules and standards, make sure that the rules and standards are clearly set out in a policy which also refers to the nature and extent of any associated monitoring. Ensure workers are aware of the policy.

It should also be made clear what action management would take in circumstances where the monitoring software identifies a problem. This in turn creates the need for managers to be trained in how the software packages work the types of problems they are designed to highlight and the appropriate courses of action to take following the identification of a possible problem.

> Any e-mail, including its content, may be monitored and used by the Information Commissioner's Office for reasons of security and for monitoring internal compliance with the office policy on staff use. E-mail monitoring/blocking software may also be used. Please be aware that you have a responsibility to ensure that any e-mail you write or forward is within the bounds of the law.

### 5.10 Cross-reference to relevant corporate policies

Organisations need to cross-reference any e-mail policy to other relevant policies, for instance the handling of confidential information, use and storage of personal data, consultation and communications at work, training, equal opportunities and harassment, and discipline and grievances at work (Acas Organisation, 2004). In addition it is important to implement a risk management policy that will incorporate e-mail retention and deletion policies, password policies, and monitoring/filtering policies. It is also necessary to incorporate the written e-mail policy into the organisation's employee handbook and new-hire orientation materials. Finally, make clear in the Acceptable Internet Use Policy that it is forbidden for employees to use a corporate e-mail address when surfing or shopping on-line.

### 5.11 Breach of e-mail policy

Generally speaking, in larger organisations the personnel/human resources department is likely to be responsible for the overall operation of the policy, making amendments as necessary, and dealing with breaches. Any breaches of the agreed policy should be addressed through the organisation's disciplinary and grievance procedures. Managers must be trained to deal with problems that might arise in e-mail and internet use.

## 6 Implementation issues and policy changes and updates

### 6.1 Implementation

Having the right e-mail policy in place is only the first step, since without proper implementation it will not effectively minimise the e-mail risks. It is important for the

e-mail policy to be related to the corporate culture of the organisation. The implementation can be undertaken gradually and is usually more difficult than writing an e-mail policy. However if people are involved in the development stage, they are much more likely to comply with the policy requirements. There are a number of practices that need to be adopted in order to accomplish a successful implementation of the e-mail corporate policy. They include how to gain the commitment of the employees as well as the managers, how to customise the policy to the needs of the organisation, and how to review, modify and communicate changes to the policy. The e-mail policy will work in cooperation with technical solutions. In order to tackle the problem of confidentiality the organisation needs to select a technical solution that allows the corporate e-mail policy to be enforced. To handle defamation and obscenity the use of content filtering software is the most obvious way of enforcing an e-mail policy, and the use of this is considered in the monitoring part of the e-mail policy.

If it is doubtful whether employees are willing to adhere to the organisation's e-mail policy and content rules this it should be taken into account in applying a technological solution to handle the problem. Policy-based content security software, working in cooperation with the e-mail policy, will monitor possible violations (ClearSwift, 2000). Finally, as part of the implementation procedure, a full explanation and clear guidance on the policy should be given to all employees in order to minimise negative impacts.

## 6.2 Updating an e-mail policy

It is important that the corporate e-mail policy to be reviewed from time to time.

The e-mail policy should include a reference such as the following.

> All personal information we collect and maintain will be subject to the version of the Privacy Policy in effect at the time of collection. We reserve the right to change the Privacy Policy from time to time and will provide notice of these changes on the home page on our web site. Please make sure you periodically review the Privacy Policy to make sure it meets your needs.

When changes or updates apply, the organisation needs to make sure that all employees are informed of the new environment.

# 7 The corporate e-mail policy for Atlantic Supermarkets SA, Greece

The corporate survey at Atlantic Supermarkets SA, Greece, titled "How employees react to spam" (see Appendix A2) provided data on employees' experience of spam, how they react to it, and whether they consider it a problem. The questionnaire was filled in by eighteen employees. All of them had internet access and corporate e-mail addresses. The following figures show the results of the questions "How many e-mails do you get on average per day at your business e-mail account?" and "What are your actions in response to spam?".

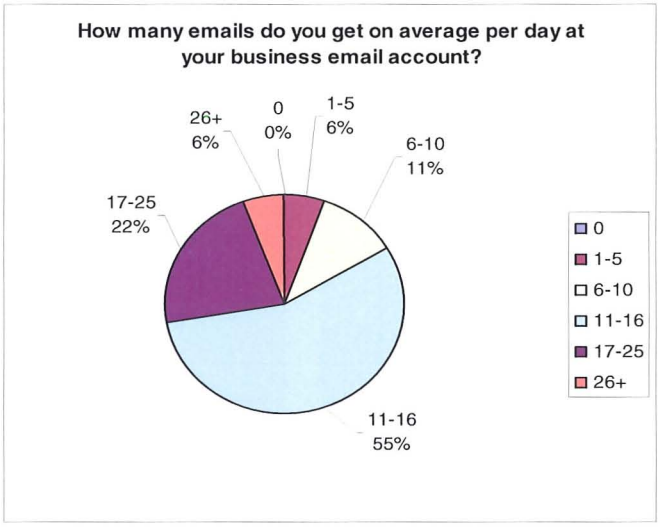



*Figure 17 – How many e-mails do you get on average per day through your business e-mail account?*

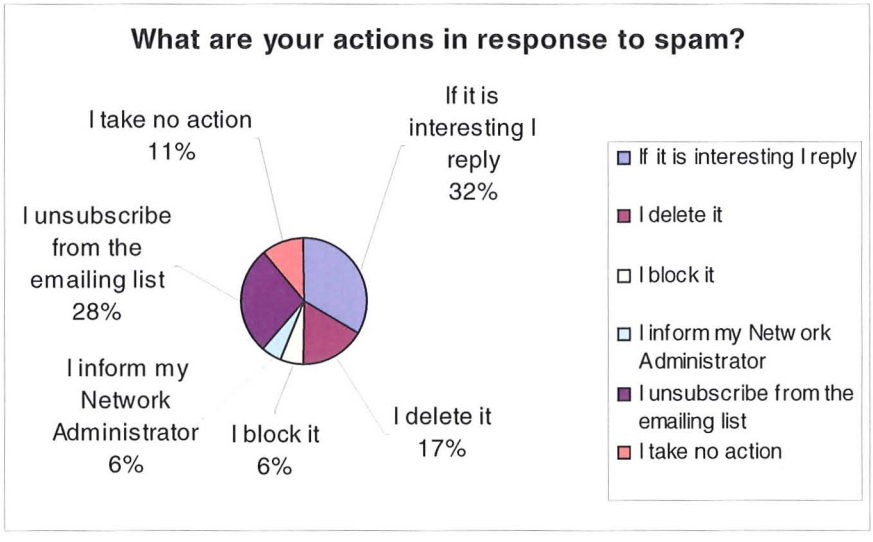



*Figure 18 – What are your actions in response to spam?*

The survey provided feedback for the development of the corporate e-mail policy for Atlantic Supermarkets.

- **Do not send sexually explicit messages, pornographic images, cartoons, or jokes.**

  Inappropriate use of the corporate e-mail and IT Systems

  Under no circumstances should the organisation's e-mail system or IT systems be used to send, receive, browse, download or store material which may be illegal, offensive or cause embarrassment to others. This includes the use of the corporate systems for: viewing, sending, receiving, downloading or distributing pornographic material or material which is racially or sexually offensive.

- **Improper content**

  Improper statements can give rise to personal or organisational liability. E-mail messages may be read by others, particularly by people who do not work within the organisation. Improper material in e-mails would offend or embarrass any such reader. Specifically: do not use defamatory statements, obscenity, slander, or libel; ethnic, sexist, religious, or racial slurs; or any other message that could be construed as harassment or disparagement of others.

- **Personal use of company facilities**

  Non-business-related e-mail use may be either completely disallowed or minimised. The minimal use of the organisation's e-mail system to send personal e-mail or to browse the World Wide Web is acceptable only if:

  (i) the usage is minimal and takes place out of normal working hours;

  (ii) the usage does not add any marginal costs to the organisation;

  (iii) the usage complies with the e-mail policy requirements.

  Do not subscribe to e-mail lists that are not job-related or company-approved. The volumes of messages that can be generated are high and you will have no control over the content.

- **Unsolicited commercial communication (spam)**

  1. Extreme care should be exercised when sending messages of any kind to multiple lists outside your organisation. This may be considered as "spamming" which is an illegal activity in many countries.

2. Do not create e-mail congestion by sending trivial messages or unnecessarily copying e-mails to those who do not have a real need to receive them.
3. Be aware what you sign up to on-line. Make sure you read the privacy policies of the site involved, since some may sell your e-mail address.
4. Be aware of check-boxes in sign-up forms that, when left unchecked, allow the company to share your information with other firms.
5. Forwarding: continuous forwarding can result in anyone being able to harvest several e-mail addresses from just one of these bulky e-mails.
6. Do not reply to spam and do not respond to messages that offer an unsubscribe option.
7. Delete, block and report junk e-mail messages.
8. Do not purchase any products through spam.

- **Identity theft**

1. Check the e-mail headers to identify who is the real sender of the e-mail.
2. Do not give personal information in an e-mail.
3. Do not share your primary e-mail address with people you know.
4. Avoid listing your e-mail address in large internet directories.

- **Phishing**

1. Do not respond to e-mails asking for security details or financial information of the organisation.
2. If you receive such an e-mail, delete it and do not open any attachments.
3. Visit banks' websites by typing the URL into the address bar.
4. Keep a regular check on your accounts.
5. Check if the web site you are visiting is secure. Also look for a lock icon on the browser's status bar.
6. Check the web address in the address bar.
7. Be cautious with e-mails and personal data.
8. Always report suspicious activity.

- **Monitoring**

  The use of office systems, including the telephone and e-mail, will be monitored. The corporate system provides the capability to monitor e-mail, voice-mail, world-wide web and other communications traffic. The organisation reserves the right to monitor e-mail, voice-mail and any other data held on its IT systems, including workstations and laptops owned by the organisation.

- **Copyrighted material**

  Always remember that text, music and other content on the internet are copyright works. Never download or e-mail such content to others unless you are certain that the owner of such works allows this.

- **Encryption and confirmation mechanisms**

  Highly confidential information should not be sent by e-mail except in encrypted form. However, users should be aware that some countries prohibit the communication of encrypted data. If sending important information by e-mail, always obtain confirmation of receipt (either a reply to your e-mail or by following up with a telephone call).

- **Using e-mail for contracting**

  Never agree to terms or enter into contractual commitments or make representations by e-mail without having obtained proper authority. Remember, when you type your name at the end of an e-mail, this act is just as much a signature as if you had signed it personally.

- **E-mail misuse**

  Think twice before opening attachments or clicking links in e-mail or instant messages, even if you know the sender. If you cannot confirm with the sender that an attachment or link is safe, delete the message. E-mail should not be used to send large attached files, unless very urgent. Many e-mail systems will not accept large files, which are returned and may result in overloading your company's own e-mail system. Exercise extreme caution when receiving attachments to e-mail messages unless you are expecting them and are certain of

the source. Be particularly wary of unusual or unexpected attachments. Executable files are the most common way that viruses are transmitted.

## 8. Summary and conclusions

In order to combat spam, organisations must integrate anti-spam technologies with corporate e-mail usage policies. An ideal anti-spam solution must personalise the corporate practices as well as individual preferences. In order for that to be achieved, there is a need for a wide range of technologies to detect spam at the gateway and a multiple, flexible and customisable policy to be applied to suspected spam messages. Ultimately, well designed and managed e-mail policies can significantly reduce the amount of spam targeting an organisation by promoting more effective internal communications. An effective e-mail policy will increase productivity by reducing the amount of time employees spend processing messages and will reduce the risk for the enterprise by minimising unacceptable messages and potential viruses. It saves money by reducing the need for e-mail processing and storage resources, as well as making messaging more useful.

# CHAPTER 9 SUMMARY, CONCLUSIONS AND FURTHER WORK

## 1. Summary

This thesis has shown that spam is an increasing problem for information society citizens. As analysed in Chapter 4, for the senders of spam getting the message to millions of people is easy and cost-effective, but for the receivers the cost is not only financial but also time-consuming, resource-consuming, possibly offensive or even illegal and sometimes dangerous to children since spam often contains pornographic material.

Although legislation has been enacted in a number of countries, it has limited impact because of the combined difficulties of crossing territorial boundaries, and of continuously evasive originating addresses. Despite the development of anti-spam technical solutions, spammers keep one step ahead. One example of that is the adaptation of subject headings to avoid filters. Filters are not effective in differentiating legitimate e-mail from spam. Additionally, if the filtering sensitivity increases, the level of spam will be reduced – but that might cause an increase in the level of legitimate e-mails that have been incorrectly tagged as spam (false positives). The research investigated options where filter control is put into the hands of individual users. Though they have the opportunity to customise and personalise filters according to their preferences, it is an unreasonable burden since it is a time-consuming process and a certain amount of expertise is required. In cases where the filter control is outsourced to knowledgeable third parties, it solves the time and knowledge problem but the cost is increased.

The initial aim of the research was to investigate the problem of spam. From that initial aim a hypothesis was formed that only a combined approach – technical, legal, corporate e-mail policy and user education – would provide a solution.

Given the inadequacy of legislation in most countries and the failure of most technical applications to resolve the problem realistically, a cooperative approach is needed. Such an approach has been developed involving all stakeholders – companies, individuals, technical developers, government and non-government organisations. Technical solutions can help but can only go so far; companies need to be aware of

the threat and be prepared ahead of time; education for consumers is needed to improve on-line behaviour and increase knowledge concerning on-line threats and vulnerabilities; and finally ISPs and other interested parties can act with law enforcement agencies to tackle spam. The following sections summarise the results of Chapters 4 and 6–8.

## 1.1 Unsolicited commercial e-mail – spam

Chapter 4 analyses the negative effect of spam and the scope of the problem. It explores the implications of UCE for the growth of global e-commerce. It specifically assesses how multiple parties such as individual users, corporations and ISPs are affected by UCE.

During the research period a new type of e-mail fraud emerged for organisations and consumers known as phishing. This new type of cyber crime has serious implications, not only for the victims but also for the success of e-commerce. Combating any criminal activity is never an easy task, and cyber crime poses its own particular problems. The consumer is an easy target in the e-commerce environment. The chapter elaborates and explains the ways in which the fraud is carried out, and how innocent users are misled by clever representations of web sites and convincing words. Additionally, it identifies specific techniques used for UCE, and suggests some preliminary approaches to addressing them.

## 1.2 Anti-spam legislation

Chapter 6 discusses how current legislative approaches can help combat spam, and specifically compares the legislative approaches in different countries. Considerable diversity exists in the legal frameworks that have been adopted by different countries around the world. The objective of the chapter is to identify, compare and contrast these divergent approaches, weigh their merits and limitations, and provide a more comprehensive view of anti-spam legislations worldwide. As argued earlier, anti-spam legislation addresses certain problems, such as intrusion into subscribers' privacy by unsolicited communications, as well as providing clear instructions for false identities or false return addresses. However, much more work must be done in order to tackle the problem. Legislation in isolation will not be able to eliminate spam. What is needed is a united approach, complemented by effective enforcement

mechanisms, cross-border cooperation, consumer and industry education, and effective implementation of advanced technical solutions. Cooperation between anti-spam groups, legislative bodies and advisory councils, direct marketing groups and ISPs is the most effective way to combat spam.

## 1.3 Technical anti-spam solutions

Technical measures (software and hardware applications) can contribute to reducing spam, but they also raise other issues. The black list approach to controlling spam is not effective since the originating address of a message can be spoofed. The use of content-filtering technologies raises the question about who decides what words are offensive, as well as whether inbound and outbound e-mail confidential information is read from unauthorised third parties during the filtering process. There have been several cases where legitimate messages were wrongly tagged as junk mail (false positives). Finally, Bayesian filters, with sufficient training, can be more effective than any other type of anti-spam filter. However, without sufficient training, the performance of Bayesian filters can be poor.

## 1.4 Organisations and corporate e-mail policy

The stakeholder analysis shows the negative impact of spam on organisations. Furthermore, a corporate survey with Atlantic Supermarkets shows that an e-mail policy could be an important element in handling spam within the organisation. Finally, the development and implementation of a corporate e-mail policy for Atlantic Supermarkets showed an improvement and reduced spam within the organisation.

Organisations, in order to combat spam, should integrate anti-spam technologies with corporate e-mail usage policies to achieve a customised and effective approach. In that case, the anti-spam solution will integrate corporate practices as well as individual preferences. A well designed and managed e-mail policy can significantly reduce the amount of spam targeting an organisation by promoting more effective communications. An effective e-mail policy will increase productivity by reducing the amount of time employees spend processing messages and will reduce the risk for the enterprise by minimising unacceptable messages and potential viruses.

## 2. Conclusions and contribution to knowledge

While e-mail has emerged as a powerful marketing tool, it has also given rise to the problem of unsolicited commercial e-mail. An exploratory analysis of UCE processes was undertaken, resulting in a typology of spam where key stakeholders were identified together with key mechanisms for addressing the problem of UCE.

At the beginning of the research, there was little or no literature in the area of spam, and no workshops, seminars or conferences. Since then, UCE has become a global problem requiring a global solution. As e-mail can originate or be routed through servers around the world, collaborative cross-national efforts to investigate and prosecute spammers have become a necessity.

The development of corporate e-policies, increased consumer and industry awareness, more sophisticated e-mail monitoring and blocking by ISPs, and better enforcement of strict legislation, are some of the key mechanisms to combat the problem of UCE.

Spam is an example of vulnerability in the internet infrastructure. The anti-spam solution also involves improving e-mail systems so that spammers will not be able to hide the origins of their e-mail messages. The key technical element for that is authentication. With an increased focus on authentication, and better understanding and enforcement of anti-spam legislation, the problem of spam can be tackled.

If spam can be stopped at the identity level and spammers start to fear criminal and civil penalties, then the problem of spam may be alleviated. Due to the insecure nature of the SMTP protocol, even records of a double opt-in confirmed subscription can be easy to fake and become unreliable as proof. One of the challenges for the implementers of legislation is to trace spammers and make sure that they are not companies that use legitimate methods to send commercial e-mail communication.

The contribution of the research is the development of a technical and legal framework based on stakeholder analysis that will eliminate spam. The framework – integrated policy and practice – reviews and critiques the current attempts at anti-spam legislation, self-regulation and technical solutions. It presents a case for an integrated user-oriented approach and provides recommendations both in IT and law.

The proposed integrated approach, involving communication among stakeholder groups, both in developing better defences against spam and in implementing those defences, constitutes the primary contribution of this research. The integrated approach will provide organisations with basic and practical advice to deal with spam issues and protect their corporate assets from cyber-fraud. This research proposes that neither legislation nor technical measures are sufficient on their own. There is no anti-spamming software package that is sufficient to tackle the problem. An e-mail blocking system is only a part of an overall effort to eliminate spam. There are a significant number of internet users that would like to receive regulated legitimate commercial communication according to their preferences. No single mechanism addressing the problem of spam – neither technical nor regulatory in nature – is likely to be successful on its own. A unified effort, combining all the key stakeholders in the UCE process, will be the most effective way to combat and manage spam.

A secondary contribution was the development of a corporate e-mail policy to handle spam. Atlantic Supermarkets SA, the tenth largest commercial enterprise in Greece and the fifth largest in its sector, was consulted, and agreed to test the e-mail policy. After the implementation of the e-mail policy, the level of spam was significantly reduced.

Chapter 6 compares legislative approaches to spam and investigates the effectiveness of each approach. The research for the anti-spam legislation is useful for its collection of references and bibliography (reviewers' comments from the 2nd Conference on E-mail and Anti-Spam, CEAS 2006, at Stanford University), for its characterisations of the various legislative approaches, and for its insights into the relative strengths and weaknesses of the various approaches.

A ccontribution to the research community was achieved by publishing a series of papers at international conferences in Europe and the USA, and by giving a number of presentations and workshops in Europe and the USA: see Appendices C and E. I was also invited as an observer-contributor to government workshops and international forums on spam in the UK (London Action Plan/DTI UK) and Belgium (EU). Finally, a number of international governmental bodies (e.g. Advisory Committee for State Informatisation (ACSI)), academic institutes (e.g. London School of Economics and Pennsylvania State University), educational portals and research papers, have

included my publications and reports as references in the area of spam (see appendices D and F).

## 3. Further work

The current research on spam will be a useful resource for customers, internet merchants, policy makers, direct marketing associations, agencies and consumer awareness groups that are working on internet security, privacy and anti-spam issues. It addresses an important and timely issue, filling an important gap in current research on e-mail marketing. It provides conceptual foundations on UCE, and deploys stakeholder analysis to suggest useful guidelines for practice.

The idea of the integrated framework includes industry self-regulation, effective and appropriate legislation, and targets enforcement against the most egregious spammers. The integrated framework indicates the need for cooperation among the major stakeholders of spam. This cooperation will involve promotion of business guidelines, best practices and technical standards that can help to tackle spam. The current research identifies spam stakeholders and recommends remedial actions that could be used as a guide. The structure given by the stakeholder analysis is a beginning in providing a foundation for researchers about issues and approaches that could be taken – both short-term and long-term – to address this problem. Spam in Japan has already taken the form of mobile SMS spam. A large percentage of text messages that Japanese mobile users receive on their cell phones is spam-related and creates a serious problem to mobile users. Despite the existence of legislation and anti-spam technology, spam is unlikely to go away in the near future. That is because the face of spam changes and e-mail attacks become more personalised based on recipients' profiles. Additionally, the majority of countries have not enacted anti-spam legislation, and as a result spammers can set up or redirect their servers through them. It can be argued that in some ways spam is more pernicious than viruses, because generally virus creators do not make money, whereas most spammers have real financial incentives. Different stakeholders need to work toward this goal through technological innovation and in partnership with other leaders in industry and government. The integrated framework was set out in a paper in the journal Internet Research (Appendix C1). This paper provides a solid conceptual foundation for future empirical research on UCE.

# REFERENCES

Acas Organisation: 2004. "Internet and e-mail policies UK".
Retrieved 11 April 2004 from http://www.acas.org.uk/about_acas/facts.html.

Accudata Systems: 2004. "Anti-spam product comparison".

Amit (Asaravala): 2003. "With this law, you can spam".
Retrieved 23 January 2004 from http://www.wired.com/news/business/0,1367,62020,00.html.

Anderson (Ross): 2001. "Security engineering: a guide to building dependable distributed systems". John Wiley.

Anti-Phishing Working Group (APWG): 2004a. "Origins of the word phishing".
Retrieved 16 November 16 from http://www.antiphishing.org/word_phish.htm.

Anti-Phishing Working Group (APWG): 2004b. "Phishing activity trends report".
Retrieved 13 September 2004 from
http://www.antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf.

Anti-Spam Monthly Review: 2003.
Retrieved August 2004 from
http://www.bigfoot.com/RUN?FN=antispamnewsletter15&locale=en#aussiespam.

AOL Inc v. Web Communications: 2000. Civil action No. 98-289A. Clerk US District Court Alexandria, Virginia.

AOL Legal Department: 2003. "Junk e-mail decisions and litigation: AOL v. Prime Data Worldnet Systems, Inc: report and recommendation".
Retrieved 1 May 2003 from http://legal.web.aol.com/decisions/dljunk/primereport.html.

Australian Government: 2003. Spam Act 2003.
Retrieved November 2004 from http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm.

Australian Government: 2004. "Australia supports anti-spam laws". News release.
Retrieved 13 January 2005 from http://www.dcita.gov.au/Article/0,,0_7-2_4011-4_118887,00.html.

Bagnall (Brian): 2000. "E-mail virus protection handbook". Syngress Media.

Bickman (Leonard) and Debra Rog: 1998. "Handbook of applied social research methods". SAGE Publications.

BiblioTech Ltd v. Sam Khuri/Benchmark: 2000.

Bolles (Gary): 2003. "Technology: spam". CIO Insight.
Retrieved 28 January 2004 from http://www.gwtools.com/gwguardian/prodlit/Technology-Spam.pdf.

BorderWare Technologies Inc: 2004. "38 e-mail security risks".
Retrieved 12 April 2004 from http://www.borderware.com/pdfs/e-mailthreats.pdf.

Boston.internet.com: 2003. "Hotmail seeks to rein-in spammers".

Retrieved 11 May 2003 from http://boston.internet.com/news/article.php/2169241.

Brightmail Inc: 2001.
Retrieved 21 May 2002 from http://www.brightmail.com.

BS 7799-2: 2002. "Information security management systems: specification with guidance for use".

Burgoyne (John): 1994. "Stakeholder analysis". In Cassel and Symon (editors): Qualitative methods in organisational research: a practical guide. Sage, New Delhi.

Burke (Brian): 2004. "Messaging security: a holistic view of anti-spam, anti-virus, policy enforcement, and regulatory compliance". IDC White Paper.

Burns (Robert): 2000. "Introduction to research methods". SAGE Publications.

Business Link, UK Government: 2005. "Introduce an internet and e-mail policy".
Retrieved 16 May 2005 from http://www.businesslink.gov.uk/bdotg/action/layer?topicId=1074402338.

Byrne (David): 2002. "Interpreting quantitative data". SAGE Publications.

Cabinet Office: 2002. "Identity fraud: a study".
Retrieved 16 April 2003 from http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf .

Cadbury Report: 2000. "The financial aspects of corporate governance". Financial Services Authority.
Retrieved 15 June 2003 from http://www.fsa.gov.uk/pubs/ukla/lr_comcode.pdf.

Can-Spam Act: 2003. Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003 (Senate).
Retrieved 11 December 2003 from
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s877enr.txt.pdf.

Canada's Business and Consumers Site: 2003. "The Canadian Code of Practice for Consumer Protection in Electronic Commerce: Preface".
Retrieved 12 April 2004 from http://strategis.ic.gc.ca/pics/ca/consumerprotection03.pdf.

Canadian Association of Internet Providers: 2002.
Retrieved 14 September 2004 from http://www.caip.ca.

Canadian Charter of Rights and Freedoms: 1982.
Retrieved 23 November 2004 from http://laws.justice.gc.ca/en/charter.

Canadian Marketing Association: 2002.
Retrieved 13 September 2004 from http://www.the-cma.org.

Caslon Analytics: 2004. "Profile: Australia and NZ spam legislation".
Retrieved 28 May 2004 from http://www.caslon.com.au/anzspamprofile2.htm.

CBC News: 2004. "Spam around the world".
Retrieved 13 September 2004 from http://www.cbc.ca/news/background/spam/world.html.

Centre for Democratic Technology (CDT): 2001. "A briefing on public policy issues affecting civil liberties online".
Retrieved 28 August 2004 from http://www.cdt.org/ publications/pp_7.04.shtml.

Centre for Democratic Technology (CDT), 2004: "Report to the Federal Trade Commission of the Ad-Hoc Working Group on UCE".
Retrieved 14 September 2004 from http://www.cdt.org/spam.

Cerf (Vinton): 2002. "Spamming is the scourge of electronic-mail and newsgroups on the internet. Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorisation."
Quoted *inter alia* at http://www.euro.cauce.org/en/index.html.

Chaffey (Dave) and P Smith: 2003. "E-marketing excellence: the heart of e-business". Elsevier Editions.

CipherTrust: 2005. "The anti spam challenge – minimising false positives".
Retrieved from http://www.cuphertrust.com/resources/articles/articles/false_positives.php.

ClearSwift: 2000. "E-security: how prepared is your business?"

ClearSwift: 2003. "Survey finds 37% of respondents have no spam policy in place".
Retrieved 12 May 2003 from http://www.mimesweeper.com/news/item.aspx? ID=206.

CNET News: 2003. "AT&T spam filter loses valid e-mail".
Retrieved 12 May 2004 from http://news.com.com/2100-1023-982118.html.

Competition Act Canada: 1985. (R.S. 1985, c. C-34).

Computer Associates Corporation: 2004. "Data Protection Guide 01 – spam: junk e-mail in the internet age".

Computer and Internet Crime: 2005.
Retrieved 13 September 2005 from http://www.cic-exhibition.com.

Consumer Guide: 2003. "Fighting spam in Australia".
Retrieved July 12, 2004 from
http://internet.aca.gov.au/acainterwr/consumer_info/spam/consumer_information/spam_consumerguide.pdf.

Coroneos (Peter): 2004. "Anti-spam initiatives in Australia". 2nd OECD Workshop on Spam.
Retrieved 11 May 2004 from http://www.oecd.org/dataoecd/8/28/33696857.pdf.

Council Decision 1999/168/EC (Annex II).

Covert (Robert): 1977. "Guidelines and criteria for constructing questionnaires". Evaluation Research Centre, University of Virginia.

CyberTrust: 2004. "No phishing: protecting employees from e-mail fraud".

Data Protection Act: 1998.

Retrieved 29 July 2004 from http://www.opsi.gov.uk/ acts/acts1998/19980029.htm.

Dearsley (Tony): 2004. Presentation at Computer and Internet Crime Conference/Exhibition. London, March 2004.
See http://www.bcs-irma.org/docs/CIC%202004%20Leaflet.pdf.

Denscombe (Martyn): 2000. "The good research guide". Open University Press.

Department of Justice Canada: 2000. Personal Information Protection and Electronic Documents Act.
Retrieved from http://www.privcom.gc.ca/legislation/02_06_01_e.asp.

Department of Justice Canada: 2002. Criminal Code (R.S. 1985, c. C-46).
Retrieved 12 February 2003 from http://laws.justice.gc.ca/en/C-46/.

Department of Trade and Industry (DTI): 2004a. "Global trio forge anti-spam pact".
Retrieved 25 March 2004 from
http://www.gnn.gov.uk/environment/detail.asp?ReleaseID=121897&NewsAreaID=2&NavigatedFromDepartment=True.

Department of Trade and Industry (DTI): 2004b. "Information security: a business guide to using the internet – step 3: develop a security policy".

Department of Trade and Industry (DTI): 2004c. "How to write an information security policy".
Retrieved 12 February 2005 from
http://www.dti.gov.uk/bestpractice/assets/ security/how_to_write_an_information_security_policy.pdf.

Department of Trade and Industry (DTI): 2004d. "Hints and tips for e-mail policy".
Retrieved from http://www.dti.gov.uk/bestpractice/assets/security/hints-tips.pdf.

Department of Trade and Industry (DTI) Business Link: 2004. "Keep your date secure".
Retrieved from
http://www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1074511455.

Dillman (Don): 2000. "Mail and internet surveys: the tailored design method". 2nd edition, John Wiley.

Direct Marketing Association (DMA): 2002.
Retrieved October 2003 from http://www.dma.org.uk.

Direct Marketing Association (DMA): 2003. "Definition of spam".
Retrieved 16 May 2003 from http://www.dmnews.com/cgi-bin/publogin.cgi?article_id=24431.

Donaldson (Thomas) and Lee Preston: 1995. "The stakeholder theory of the corporation: concepts, evidence, and implications". Academy of Management Review, volume 20 number 1 pages 65-91.

EEMA: 2002.
Retrieved 14 May 2002 from http://www.eema.org.

E-mail Marketing Conference, Chicago: 2004.
Retrieved from http://e-mailuniverse. com/list-news/?id=996.

EnTrust Co: 2005. "Countering on-line identity theft: new tools to help battle identity theft on the internet".

e-Policy Institute: 2004. "The potential for messy, costly e-crises is huge!"
Retrieved 16 November 2004 from http://www.epolicyinstitute.com/disaster/stories.html.

e-Security uncovered: 2005. Williams F1 Conference Centre.
Retrieved from http://www.esu.gsec.co.uk.

EU Brussels Workshop: 2003. "Unsolicited commercial communications".
Retrieved 2 August 2004 from
http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm.

EU Business: 2005. "Spam".
Retrieved 13 May 2005 from http://www.eubusiness. com/guides/spam.

EU Directive 2002/58/EC: 2002. "Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications)".
Retrieved 23 January 2004 from
http://europa.eu.int/eur-lex/pri/en/oj/ dat/2002/l_201/l_20120020731en00370047.pdf.

EU Report IP/03/1373. "Spam: Commission discusses with public and private stakeholders how to fight spam".

EUROPA: 2001. "Junk e-mail costs internet users €10 billion a year worldwide".
Retrieved 24 February 2003 from
http://europa.eu.int/ISPO/docs/ services/docs/2001/February/ip_01_154_en.pdf.

European Commission: 2003. "Internet subscribers world-wide are unwittingly paying an estimated €10 billion a year in connection costs just to receive 'junk' e-mails, according to a study undertaken for the EU".
Retrieved 11 December 2003 from http://europa.eu.int/comm/internal_market.

European Corporate Governance Institute (ECGI): 1992.
Retrieved 13 August 2003 from http://www.ecgi.de/codes/.

European Parliament and Council: 2002. "Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector".
Retrieved 13 May 2003 from
http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

EuroUnion: 2003. "Spam: European Commission goes on the offensive".
Retrieved 15 July 2003 from http://www.eurunion.org/News/press/2003/2003044.htm.

Federal Court of Australia (FCA): 2006. Australian Communications and Media Authority v Clarity1 Pty Ltd. FCA 410.

Federal Trade Commission (FTC): 2002. "You've got spam: how to 'can' unwanted e-mail".
Retrieved 2 September 2003 from http://www.ftc.gov/bcp/conline/pubs/ online/inbox.pdf.

Federal Trade Commission (FTC): 2003. "FTC measures false claims inherent in random spam".
Retrieved 9 February 2004 from http://www.ftc.gov/opa/2003/ 04/spamrpt.htm.

Federal Trade Commission (FTC): 2005. "The US Safe Web Act: protecting consumers from spam, spyware, and fraud; a legislative recommendation to Congress".

Financial Services Technology Consortium (FSTC): 2004. "Counter-phishing initiative".
Retrieved 15 October 2004 from http://www.antiphishing.org/ FSTC_Phishing _Prospectus_Final.pdf.

Finley (Michelle): 2000. "Phone phreaks to rise again?"
Retrieved from http://www.wired.com/ news/print/0,1294,36309,00.html.

Flynn (Nancy): 2000. "The e-policy handbook: designing and implementing effective e-mail, internet, and software policies". AMACOM/American Management Association.

Flynn (Nancy): 2003. "E-mail rules". E-Policy Institute.

Foddy (William): 1994. "Constructing questions for interviews and questionnaires". Cambridge University Press.

Forsite Group: 2004. "Use or abuse? Why your company needs a web policy".

Freeman (R Edward): 1984. "Strategic management: a stakeholder approach". Pitman.

Gartner Group: 2001.
Retrieved 21 August 2002 from http://www4.gartner.com/Init.

Gartner Group: 2003. "Gartner says marketers must differentiate e-mail marketing from spam". Press release.
Retrieved 29 March 2003 from http://www4.gartner.com/ 5_about/press_releases/pr29sept2003a.jsp.

Gellman (Robert): 2002. "How the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete". Electronic Privacy Information Center, Washington DC.

Gengler (Charles) and Thomas Reynolds: 1995. "Consumer understanding and advertising strategy: analysis and strategic translation of laddering data". Journal of Advertising Research.

Gerard (Philippe): 2005. "Cooperating internationally against spam". 4th Conference on e-Commerce: Tackling Spam.

GFI: 2004. "Why Bayesian filtering is the most effective anti-spam technology".
Retrieved 18 November 2004 from http://www.gfi.com/whitepapers/why-bayesian-filtering.pdf.

Godin (Seth): 1999. "Permission marketing: turning strangers into friends, and friends into customers". Simon & Schuster.

Grabarek (Bill): 2004. "FTC: do-not-spam not the answer". Direct Newsletter.

Gradwell (Peter): 2003. InternetWorld Journal.

Graham (Paul): 2002. "A plan for spam".
Retrieved 17 September 2003 from http://www.paulgraham.com/spam.html.

Greene (Maxine): 1988. "The dialectic of freedom". Teachers College Press.

Group Technologies Corporation: 2005. "Why do anti-spam policies make sense?"
Retrieved 22 June 2005 from http://www.group-technologies.com/en/products/ faq/antispam.php.

Grunert (Klaus): 1996. "Automatic and strategic processes in advertising effects". Journal of Marketing, volume 60 number 4 pages 88-100.

Guba (Egon) and Yvonna Lincoln: 1994. "Competing paradigms in qualitative research". In Denzin and Lincoln (editors): Handbook of Qualitative Research. Sage.

Haftke (Mark): 2002. "A practitioner's guide to the regulation of the internet". 2nd dition, Legal City and Financial Publishing.

Hailey (Gary): 2004. "Congress urges FTC to crack down on spammers". Legal Review – Response Magazine.

Hamiltons Solicitors: 2003. "Legal update".
Retrieved 2 June 2004 from http://www.hamiltons-solicitors.co.uk/archive-docs/legal%20update.htm.

Hance (Olivier) and Suzanne Balz: 1997. "Business and law on the internet". McGraw-Hill.

Harbaugh (Logan): 2004. "Rival solutions smack down spam". InfoWorld.

Harris (David): 2003. "SPAM, the curse of the new millennium: an overview and white paper".

Heeger (David): 1997. "Signal detection theory". Department of Psychology, New York University.
Retrieved from http://www.cns.nyu.edu/~david/sdt/sdt.html.

Higa (K), O Sheng, B Shin and A Figeuredo: 2000. "Understanding relationships among teleworkers' e-mail usage, e-mail richness perceptions and e-mail productivity perceptions under a software engineering environment". IEEE Transactions on Engineering Management.

Hollis (Richard): 2003. "ORTHUS information security solution". EEMA Conference, Dublin.

Horton (Robert): 2004. "ITU WSIS Thematic Meeting on Countering Spam": Report. World Summit on the Information Society, Geneva.
Retrieved from http://www.itu.int/osg/spu/spam/chairman-report.pdf.

Hoxmeier (John) and Winter Nie: 2000. "The impact of gender and experience on user confidence in electronic mail". Journal of End-User Computing.

Identity Theft Resource Centre: 2004. "Identity theft facts and statistics".
Retrieved from http://www.idtheftcenter.org/facts.shtml.

IDG News Service: 2001.
Retrieved 12 February 2002 from http://lists.essential.org/pipermail/ecommerce/2002q1/000656.html.

Industry Canada: 1997. "Spam discussion paper – internet and bulk unsolicited electronic mail".
Retrieved 13 October 2002 from
http://e-com.ic.gc.ca/epic/internet/inecicceac.nsf/vwapj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf.

Industry Canada: 2003. "Spam discussion paper – e-mail marketing: consumer choices and business opportunities".
Retrieved from http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00170e.html.

Industry Canada: 2004. "Task Force on Spam: round-table meeting with key stakeholders".
Retrieved 26 May 2005 from http://blog.cauce.ca/blog/archives/ Taskforce_Roundtable.pdf.

Industry Canada: 2005. "Stopping spam, creating a stronger safer internet".

Information Security Magazine: 2000. "Pulling the plug on surfing and spam".
Retrieved 1 May 2002 from http://infosecuritymag.techtarget.com/articles/april00/features1. shtml.

Institute of Chartered Accountants in England and Wales: 2005. "Review of the Turnbull Guidance".
Retrieved 14 October 2002 from http://www.icaew.co.uk/internalcontrol.

International Data Corporation (IDC): 2000.
Retrieved 13 March 2002 from http://www.idcresearch.com.

International Telecommunication Union: 2003. "Geneva declaration of principles": paragraph 37. World Summit on the Information Society 2003, Geneva.
Retrieved from http://www.itu.int/wsis/docs/geneva/official/dop.html.

Internet World Statistics: 2005.
Retrieved 30 April 2005 from http://www. internetworldstats.com.

ISO/IEC 17799: 2000. "Information technology – code of practice for information security management".

Jackson (T), R Dawson and D Wilson: 2003. "Understanding e-mail interaction increases organisation productivity". Communications of the ACM, volume 46 number 8 pages 80-84.

JNUG (JANET National User Group): 2005. "JNUG Netiquette and junk mail".
Retrieved 5 December 2005 from http://www.jnug.ac.uk/reports/jmail.html.

Jones (Phil): 2003. EEMA Conference, Dublin.

Khong (Dennis): 2004. "The problem of spam law: a comment on the Malaysian Communications and Multimedia Commission's discussion paper on regulating unsolicited commercial messages". Computer Law and Security Report, volume 20 number 3 pages 206-212.

Kille (Steve): 2003. EEMA Conference Spam – death of e-mail?

Knight (William): 2004. "Goin' phishing?" Conference Infosecurity Today.

Koppanyi (Szabolcs): 2003. EEMA Conference, Dublin.
Retrievd from http://goliath.ecnext.com/coms2/summary_0199-1306758_ITM.

Krim (Jonathan): 2003. "Spam's cost to business escalates". Washington Post, 13 March 2003 page A01.

Krishnamurthy (Sandeep): 2000. "Spam revisited". Quarterly Journal of E-Commerce', volume 1 number 4 pages 305-321.

Langford (Duncan): 2000. "Internet ethics". Macmillan.

Law Society: 2004. "E-mail guidelines for solicitors".

Law Society: 2005. "E-mail guidelines for solicitors".
Retrieved 6 April 2005 from http://www.lawsociety.org.uk/documents/downloads/emailguidelines.pdf.

Lee (Allen): 1994. "Electronic mail as a medium for rich communication: an empirical investigation using hermeneutic interpretation". MIS Quarterly, volume 18 number 2 pages 143-157.

Liikanen (Erkki): 2003. "Spam: European Commission goes on the offensive".
Retrieved 4 May 2004 from http://www.eurunion.org/News/press/2003/2003044.htm.

Maanen (John): 1984. "Qualitative methodology". Sage.

MailFrontier: 2004a. "MailFrontier research survey detects slowdown in online holiday shopping".
Retrieved 18 November 2004 from http://www.mailfrontier.com/press/press_holidays.html.

MailFrontier: 2004b. "Phishing IQ test II".
Retrieved 13 November 2004 from http://survey.mailfrontier.com/survey/quiztest.html.

MailWasher: 2001a.
Retrieved 22 November 2001 from http://www.mailwasher.net.

MailWasher: 2001b. "MailWasher Software Report". Web User Magazine.
*"More than 98% of computer viruses now arrive via spam, cleverly camouflaged with introductory messages like 'I love you' or tempting picture attachments of Britney Spears, Madonna or Anna Kournikova. The Melissa virus was significant in that it was the first major example of spam effectively 'hijacking' the user's computer."*

MAPS Realtime Blackhole List (RBL): 2001.
Retrieved 12 September 2002 from http://www.mail-abuse.org.

McManus (Denise), Chetan Sankar, Houston Carr and F Nelson Ford: 2002. "Intraorganisational versus interorganisational uses and benefits of electronic mail". Information Resources Management Journal, volume 15 number 3 pages 1-13.

Meade (Joe): 2003. "Spam – the death of e-mail?" EEMA Conference, Dublin.

Metchis (Hanah) and Solveig Singleton: 2003. "Spam, that ill o' the ISP: a reality check for legislators". Competitive Enterprise Institute.
Retrieved from http://www.cei.org/pdf/3482.pdf.

Milne (George) and Mary Gordon: 1993. "Direct mail privacy–efficiency trade-offs within an implied social contract framework". Journal of Public Policy and Marketing, volume 12 number 2 page 206.

Ministry of Internal Affairs and Communications (Japan): 2003.
Retrieved 12 March 2003 from http://www.soumu.go.jp/english/index.html and
http://www.soumu.go.jp/joho_ tsusin/top/pdf/meiwaku_01.pdf (Japanese Version).

Ministry of Public Management, Home Affairs, Posts and Telecommunications (Japan): 2003.
Retrieved from
http://www.itu.int/ITU-D/treg/Events/Seminars/Virtual-events/Spam/Spam-MPHPT.pdf.

Mitchell (Ronald), Bradley Agle and Donna Wood: 1997. "Towards a theory of stakeholder identification: defining the principle of who and what really counts". Academy of Management Review, volume 22 number 4 pages 853-886.

Miyake (Kuriko): 2001. IDG News Service, Tokyo Bureau.

Monty Python sketch: 1970.
Retrieved 27 May 2002 from http://bau2.uibk.ac.at/sg/python/Scripts/TheSpamSketch.

NASCIO: 2005. "Welcome to the jungle: the State privacy implications of spam, phishing and spyware".

National Technology Readiness Survey: 2004. "Summary report" by Rockbridge Associates Inc.
Retrieved 14 June 2005 from http://www.rhsmith.umd.edu/ntrs/ NTRS_2004.pdf.

NetworkWorldFusion: 2003. "Math to fight spam".
Retrieved 21 May 2004 from http://www.nwfusion.com/columnists/2003/0922gearhead.html.

Ngwenyama (Ojelanki) and Allen Lee: 2002. "Communication richness in electronic mail: critical social theory and the contextuality of meaning". MIS Quarterly, volume 21 number 2 pages 145-168.

NHTCU (National Hi-Tech Crime Unit): 2004. "13 internet fraudsters arrested by National Hi-Tech Crime Unit". Press statement.

Nucleus Research: 2003. "Spam: the silent ROI killer": Research Note D59.
Retrieved from http://www.nucleusresearch.com/research/d59.pdf.

OECD: 2004. "Anti-spam legislation and authorities: country profiles – Australia".
Retrieved 28 April 2005 from
http://www.oecd.org/document/55/0,2340,en_2649_22555297_34409847_1_1_1_1,00.html.

OECD Task Force on Spam: 2005. "Spam issues in developing countries". DSTI/CP/ICCP/SPAM(2005)6/FINAL.

OECD Work on Spam: 2004a.
Retrieved 30 May 2004 from
http://www.oecd.org/ department/0,2688,en_2649_22555297_1_1_1_1_1,00.html.

OECD Work on Spam: 2004b.
Retrieved 24 June 2005 from http://www.oecd.org/sti/spam/.

OECD Work on Spam: 2005. "Country: New Zealand".
Retrieved 24 June 2005 from
http://www.oecd.org/document/31/0,2340,en_2649_22555297_34417119_1_1_1_1,00.html.

Office of Fair Trading: 2004. "London action plan on spam".
Retrieved 29 January 2005 from http://www.oft.gov.uk/News/Press+releases/2004/168-04.htm.

Office of the Privacy Commissioner (New Zealand): 2002. "Catching the fast slithering tail of e-privacy".
Retrieved 17 May 2003 from http://www.privacy.org.nz/top.html.

Overton (Martin): 2004. "Canning more than spam with Bayesian filtering". Virus Bulletin Conference 2004.

PC Advisor: 2004. "Anti-spam security products".

Pendharkar (Parag) and Karl Young: 2004. "The development of a construct for measuring an individual's perceptions of e-mail as a medium for electronic communication in organisations". IEEE Transactions on Professional Communication, June 2004 pages 130-143.

Postel (Jonathan): 1982. "Simple Mail Transfer Protocol".
Retrieved 1 May 2004 from http://www.ietf.org/rfc/rfc821.txt.

Radio Singapore International: 2003.
Retrieved 16 November 2004 from http://rsi.com.sg/english/undertones/view/2004031615551/1/.html.

Realtime Blackhole List (RBL): 2002.
Retrieved 4 October 2002 from http://www.mail-abuse.org.

Reed (Christopher): 2003. "Internet law: text and materials". Butterworths.

Robinson (Gary): 2003. "A statistical approach to the spam problem". Linux Journal.
Retrieved from http://www.linuxjournal.com/article/6467.

Rosenoer (Jonathan): 1996. "Cyberlaw the law of the internet". Springer.

Sahel (Jean-Jacques): 2005. "Spam as a vehicle for transnational criminal menace – but solutions are looming". ASEM 4th Conference on e-Commerce Tackling Spam.
Retrieved 19 September 2005 from http://www.asemec-london.org.

Schneider (Kenneth): 2004. "Threats to e-mail security". EU Workshop on Spam: public consultation and workshop on combating spam. Symantec.

Sheatsley (Paul): 1983. "Questionnaire construction and item writing." In Rossi, Wright and Anderson (editors): Handbook of Survey Research: Quantitative Studies in Social Relations, pages 195-230. Academic Press.

Shiels (Maggie): 2002. "Why one spam could cost $50". wBBC News.
Retrieved 12 May 2003 from http://news.bbc.co.uk/1/hi/sci/tech/1917458.stm.

Sipior (Janice), Burke Ward and P Gregory Bonner: 2004. "Should spam be on the menu?" Communications of the ACM, volume 47 number 6 pages 59-64.

Somekh (Bridget) and Cathy Lewin: 2005. "Research methods in the social sciences". SAGE Publications.

Spamhaus: 2004a. "SBL blocklist rationale".
Retrieved 17 June 2004 from http://www.spamhaus.org/sbl/sbl-rationale.html.

Spamhaus: 2004b. "Follow Australia!"
Retrieved 11 July 2004 from http://www.spamhaus.org/news.lasso?article=154.

SpamLaws: 2003.
Retrieved 17 September 2002 from http://www.spamlaws.com/ federal/108s877enrolled.pdf.

Spinello (Richard): 1999. "Ethical reflections on the problem of spam". Springer.

Stratton Oakmont Inc v Prodigy Services Co: 1995. 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. May 24, 1995).
Retrieved from http://www.tomwbell.com/NetLaw/Ch04/Stratton.html.

Sturdevant (Cameron): 2003. "Anti-spam law has holes".
Retrieved from http://www.eweek.com/article2/0,1895,1407895,00.asp.

Sudman (Seymour), Norman Bradburn and Norbert Schwarz: 1995. "Thinking about answers: the application of cognitive processes to survey methodology". Jossey-Bass.

SurfControl: 2003. "The managers' e-mail guide".
Retrieved from http://www.surfcontrol.com/uploadedfiles/how_to_write_an_email_aup_uk.pdf.

Symantec: 2004. "EU Workshop on Combatting Spam" (Brussels).

Turban (Efraim), Jae Lee, David King and H Michael Chung: 2000. "Electronic commerce: a managerial perspective". Prentice-Hall.

UK Anti-spam Law, 2003 Consumer Protection (Unsolicited E-mails).
Retrieved 11 November 2004 from
http://www.parliament.the-stationeryoffice.co.uk/pa/ cm200203/cmbills/119/2003119.htm.

United Nations Conference on Trade and Development (UNCTAD): 2003a. "E-commerce and development report". Chapter 1: "Recent internet trends: access, usage and business applications".
Retrieved 29 October 2003 from http://www.unctad.org/en/docs/ecdr2003ch1_en.pdf.

United Nations Conference on Trade and Development (UNCTAD): 2003b. "E-commerce and development report". Chapter 3: "ICT strategies for development".
Retrieved from http://www.unctad.org/en/docs/ecdr2003ch3_en.pdf.

University of Houston (2005). "Phishing scams".
Retrieved 12 June 2005 from http://www.uh.edu/infotech/news/story.php?story_id=802.

US Department of Homeland Security: 2004. "Avoiding social engineering and phishing attacks".
Retrieved 21 June 2005 from http://www.us-cert.gov/cas/ tips/ST04-014.html.

US Federal Trade Commission: 2003. "ID theft: what it's all about".
Retrieved 30 June 2004 from http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm.

Veendal (Gert): 2003. Quoted in Whittle (Sally): "Full up". Internet World.
Retrieved from
http://www.internetworld.co.uk/london/magazine/index.cfm?fuseaction=article&ArticleID=365.

VB2004 Conference: 2004. 14th Virus Bulletin International Conference: Chicago.

Wall (David): 2004. "Can we can the spam?" Computers and Law, volume 14 issue 6.

Walrave (Michel): 2003. "Cyberkids' e-privacy at stake? data processing and privacy policies in websites aimed at minors": Privacy Paper 4. University of Antwerp Communication Studies.

Weber (Ron): 2004. "The grim reaper: the curse of e-mail". MIS Quarterly. volume 28 number 3 pages iii-xiii.

Wood (Paul): 2003. "A spammer in the works: everything you need to know about protecting yourself and your business from the rising tide of unsolicited 'spam' email". MessageLabs White Paper.
Retrieved from http://www.security.iia.net.au/downloads/aspammerintheworks.pdf.

Yale Law School: 2003. "Spam laws worldwide: Japan".
Retrieved 1 May 2003 from
http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1326.

York (Stephen) and Kenneth Chia: 2002. "E-commerce: a guide to the law of electronic business". Butterworth.

Zixcorp: 2003. "Spam filters need the human touch": white paper.

# APPENDIX A QUESTIONNAIRES

## 1 How users react to spam

Old version **Unsolicited Commercial Communication (spam)**

This is a survey regarding Unsolicited Commercial Communication also known as spam in e-mail communication. Your views will provide valuable feedback for the PhD research. Thank you for your co-operation! ☺
Evangelos Moustakas (PhD Researcher Middlesex University) e.moustakas@mdx.ac.uk

**A) About you**
Current Location (country):
Gender:
Age Group: 15-18, 19-25, 26-35, 36-45, 46-55, 55+

**B) Your access to the Internet**

**Where do you access the Internet?**
a) Work.....
b) Home.....
c) University.....
d) Cyber Café.....
e) Other (please specify).....

(You may tick more than one)

**What type of Internet connection do you have?**
a) Dial Up.....
b) Broadband.....
c) ISDN.....
d) Other (please specify)....

**What Internet Service Provider do you use to access the web?**
a) BT.....
b) AOL.....
c) Free Serve.....
d) Other (Please specify)....

**Have you set up an e-mail account with this provider?**
a) Yes.....
b) No.....

**Which web-e-mail service do you use?**
a) Hotmail.....
b) Yahoo.....
c) Icqmail.....
d) Other (please specify)....
e) None.....

**C) Your E-mail + Unsolicited Commercial Communication**

**How many unsolicited e-mails do you get on average per day using your ISP's e-mail account?**
e) None.....
b) –5.....
c) 6-10.....
d) 11-16.....
e) 17-25.....
f) 25+.....

**How do you consider spam?**
a) Interesting.....
b) A nuisance.....
c) Harmful.....
d) No strong feelings about it.....

**Have you got anti-spamming software running on your pc?**
a) Yes.....
b) No.....
c) I don't know.....

**If you use a web e-mail service, how many unsolicited e-mails do you get per day?**
a) None.....
b) -5.....
c) 6-10.....
d) 11-16.....
e) 17-25.....
f) 25+.....

*D) Your views*

**What are your actions in response to spam?**
a) I delete it.....
b) I block it.....
c) I inform my Internet Service Provider.....
d) I unsubscribe from the e-mailing list .....
e) I take no action.....

**Would you be willing to pay an additional fee to your ISP if it provides the guarantee for spam free e-mail service?**
a) Yes.....
b) No.....
c) I don't think it's important.....

**Who do you think, from the following stakeholders, is the most appropriate to handle spam?**
a) The ISP.....
b) The Government (legislation).....
c) Marketing Associations.....
d) The user.....
e) Other (please specify).....

Final version Unsolicited Commercial Communication (spam)
This is a survey regarding Unsolicited Commercial E-mail also known as spam in e-mail communication. Your views will provide valuable feedback for the PhD research. Thank you for your co-operation! Evangelos Moustakas (PhD Researcher Middlesex University) e.moustakas@mdx.ac.uk

**A) Your access to the Internet**

**1. What type of Internet connection do you have?**
a) Dial Up.....
b) Broadband.....
c) ISDN.....
d) Other (please specify)....
(Tick one box only)

**2. What Internet Service Provider do you use to access the web?**
a) BT.....
b) AOL.....
c) Free Serve.....
d) Other (Please specify)....
(Tick one box only)

**3. Have you set up an e-mail account with this provider?**
a) Yes.....
b) No.....

**4. Which web-e-mail provider do you use?**
a) Hotmail.....
b) Yahoo.....
c) Icqmail.....
d) Other (please specify)....
e) None.....
(You may tick more than one)

**B) Your E-mail + Unsolicited Commercial Communication**

**1. How many e-mails do you get on average per day using your ISP's e-mail account?**
e) None.....
b) –5.....
c) 6-10.....
d) 11-16.....
e) 17-25.....
f) 25+.....

**2. How many of the above e-mails are spam?**
e) None.....
b) –5.....
c) 6-10.....
d) 11-16.....
e) 17-25.....
f) 25+.....

**3. Was an anti-spam filter included in the ISP's e-mail account or did you install it by yourself?**
a) Provided by ISP
b) I installed it myself
c) I don't have anti-spam software
d) I don't know
(Tick one box only)

**4. How many e-mails do you get on average per day using web-e-mail account?**
a) None.....
b) -5.....
c) 6-10.....
d) 11-16.....
e) 17-25.....
f) 25+.....

**5. If you use a web e-mail service, how many unsolicited e-mails do you get per day?**
a) None.....
b) -5.....
c) 6-10.....
d) 11-16.....
e) 17-25.....
f) 25+.....

*C) Your views*

**1. How do you consider spam?**
a) Interesting.....
b) A nuisance.....
c) Harmful.....
d) Undecided.....
(Tick one box only)

**2. What are your actions in response to spam?**
a) I delete it.....
b) I block it.....
c) I inform my Internet Service Provider.....
d) I unsubscribe from the e-mailing list .....
e) I take no action.....
(Tick one box only)

**3. Would you be willing to pay an additional fee to your ISP if it provides the guarantee for spam free e-mail service?**
a) Yes.....
b) No.....
c) Undecided.....

**4. Who do you think is the most appropriate to handle spam?**
a) The ISP.....
b) The Government (legislation).....
c) Marketing Associations.....
d) The user.....
e) Other (please specify).....
(You may tick more than one)

**D) About you**

1. **Current Location** (country):
2. **Gender**:
3. **Age Group**: 15-18, 19-25, 26-35, 36-45, 46-55, 55+

## 2. Atlantic Supermarkets

1. Do you have a corporate e-mail address (e.g. name@atlantic.gr)?
a) Yes
b) No

2. How many e-mails do you get on average per day at your business e-mail account?
a) None.....
b) –5.....
c) 6-10.....
d) 11-16.....
e) 17-25.....
f) 25+.....

3. How many of the above e-mails are spam?
a) None.....
b) –5.....
c) 6-10.....
d) 11-16.....
e) 17-25.....
f) 25+.....

4. How do you consider spam?
a) Interesting.....
b) A nuisance.....
c) Harmful.....
d) Undecided.....
(Tick one box only)

5. What are your actions in response to spam?
a) If it is interesting I reply.....
b) I delete it.....
c) I block it.....
d) I inform my Network Administrator.....
e) I unsubscribe from the e-mailing list .....
f) I take no action.....

6. Which web-e-mail provider do you use?
a) Hotmail.....
b) Yahoo.....
c) Icqmail.....
d) Other (please specify)....
e) None.....
(You may tick more than one)

7. Are you checking your personal e-mail from work?
a) Yes
b) No

# APPENDIX B INTERVIEWS

The same questions were used for all interviews. They are reproduced below only for P. Jones.

## 1 Phil Jones, UK Data Protection Commissioner (Privacy and Spam), 10 February 2004

### Agenda

1. The implementation of the EU Directive differs between the Member States. Could you identify differences between the Member States?

   Some National Laws (e.g. Spain) had already introduced the 'opt-in' regime for e-mail before the Directive of 2002. Other National Laws transposed the Directive but 'modified' the concept of 'opt-in' (e.g. Denmark) and several Member States transposed the Directive only partially (e.g. Belgium). Finally a large number of Member States have not yet transposed the Directive (e.g. France, Germany). There are a number of divergences between Member States such as whether the Directive applies to natural and/or legal persons, whether the requirements for consent are oral/written, explicit/implicit, active/passive, and who manages the opt-in/opt-out mailing lists. Harmonisation among the Member States is the desirable objective but also a very difficult task.

2. Which law is applicable if a UK-based company sends unsolicited e-mail to Greece and vice-versa?

   If both sender and recipient are companies, sending spam is not illegal. If the recipient is an individual he can complain to the sender's ISP or the Marketing Association. The recipient in Greece may sue the sender in the UK, and the court will take place in the UK.

3. The effectiveness of the EU Directive is small since most spam originates from outside the EU.

   When a consumer is interested in a specific product or service the consumer will have to request information from relevant companies. Although there will be an awareness of the larger companies, the consumer is unlikely to know many small and medium size companies who offer similar products/services at competitive prices. This results in a reduction of market competition and a reduction in consumer choice. Unfortunately we have not yet seen any e-mail contain a statement that it is a 'commercial e-mail' or 'unsolicited commercial e-mail' as required by the Electronic Commerce Directive.

4. CAN-Spam Act 2003 – EU Directive 2002 Harmonisation?

   Global Harmonisation is very difficult since the USA and the EU have opt-out / opt-in regimes. Despite this variation, in the future we may see that the

requirements for sending Commercial Communication around the world will be similar. For example when the e-mail contains pornographic material only a URL link should be included in the body of the message and in addition the subject line of the e-mail should indicate that the message is pornographic.

5. ISPs responsibilities

   - Review Contractual agreements between users and ISPs.
   - False positives - Loss of legitimate e-mail.
   - Sending e-mail to wrong recipients.

6. How can we tackle the problem of spam? The integrated scenario

   The idea of the integrated scenario that I introduced in the IFIP Conference in Sweden is considered as the most effective method to tackle spam. According to Commissioner Liikanen (OECD Workshop on Spam, 2-3 February 2004), an OECD framework should aim to promote:

   - An *effective 'anti-spam' law* in all countries;
   - *Cross-border cooperation* on enforcement in specific cases;
   - *Self-regulatory solutions* by market players e.g. on contractual and marketing practices;
   - *Technical solutions* to manage or reduce spam, like filtering and other security features;
   - Greater *consumer awareness* about, e.g., how to minimise spam and how to react to spam and complain.

## 2 Professor Dr Michel Walrave, Catholic University of Leuven, 19 February 2004

Professor Walrave conducted a survey on on-line data processing and unsolicited commercial e-mail. During the meeting we reviewed the questionnaire of my survey and we made a small number of changes. He provided me with feedback from his survey and we examined different methods for evaluating data coming from surveys.

## 3 Philippe Gerard, DG Information Society, European Commisssion, 19 February 2004

The outcomes of the interview were as follows.

- Spam affects everyone. The solution should be global. The idea of the integrated Scenario Enforcement is very difficult but crucial.
- The problem of spam is multi-faceted and it will be very hard to tackle in the near future.

- Though harmonisation needs to be, and can be, achieved among the EU Member States and countries, it is a very complicated and time-consuming task.
- The year 2006 is considered as the year for reviewing the Directive of 2002 about spam.
- Cookies, Online e-mail policies and Terms and Conditions for On-line Contracts are very much related to spam.

# APPENDIX C PUBLICATIONS

1. Evangelos Moustakas, C. Ranganathan, Penny Duquenoy (2006) E-mail marketing at the crossroads: A stakeholder analysis of unsolicited commercial e-mail (spam)'. **Internet Research**, Vol 16(1), 38-52.

   The purpose of this paper was to provide a conceptual overview of the process of unsolicited commercial e-mail (UCE), propose a typology of UCE, and delineate key stakeholders of UCE, their roles and potential responses through a stakeholder analysis. Based on the extant literature, this paper provided a conceptualisation of the UCE process, delineating specific types of UCE. It used stakeholder analysis to identify key members in the UCE process and the potential roles to be played by them in combating UCE. The paper proposed a four-way typology of the UCE process, identified key stakeholders, and also mechanisms for tackling UCE.

2. Evangelos Moustakas, C. Ranganathan, Jean-Jacque Sahel, Michel Walrave, Lynn Voss, Ana Branca Carvalho. Use of Corporate E-mail Policies for Combating Unsolicited Commercial Communications: Towards Development of a Framework. **International Conference on Information Warfare and Security (ICIW 2006)** University of Maryland Eastern Shore, USA [http://www.academic-conferences.org/iciw/iciw2006/iciw06-home.htm] (15-16 March 2006)

   In order to combat the spread of unsolicited e-mails at workplace, several organisations are increasingly implementing corporate policies and employee Acceptable Use Policies (AUPs). Further, organisations enforce these policies by implementing technical solutions. This paper explored the risks involved in unsolicited mails at a work environment and analyzed the effectiveness of corporate e-mail policies in minimizing spam. Drawing upon organisational experiences, we developed a framework for designing appropriate corporate e-mail policies for combating spam. We focused on the formulation as well as implementation aspects of corporate policies for combating spam. Finally, based on real world case studies, we outlined a set of suggestions and recommendations for devising corporate e-mail policies.

3. Evangelos Moustakas, C. Ranganathan, Ana Branca Carvalho (2005) 'Abort, delete, or ignore? Assessing the implications of unsolicited commercial communication (spam) for e-commerce' **IADIS International Conference e-Commerce 2005**, Porto, Portugal [http://www.iadis.org/ec2005] (15-17 December 2005)

   This paper explored the implications of UCE for the growth of global e-commerce, specifically assessing how multiple parties such as individual users, corporations and internet service providers are affected by UCE. Specific spam techniques were analyzed and some suggestions to address the problem of UCE were provided.

Although e-mail has proved to be an effective marketing tool, its misuse could potentially erode its appeal, popularity and usage, as well as pose a fundamental threat to consumer confidence in e-commerce. Unsolicited Commercial Communication (UCE), commonly known as spam, impinges on the privacy of individual Internet users. It can also cost users in terms of the time spent reading and deleting the messages, as well as in a traditional economic sense where users pay time-based connection fees. Moreover, the problem of spam also extends into the realm of corporations as precious technology resources and employee hours can be affected by UCE.

4. Evangelos Moustakas, C. Ranganathan, Penny Duquenoy (2005) 'Combating Spam through legislation: A Comparative Analysis of US and European Approaches' **2nd Conference on E-mail and Anti-Spam (CEAS 2005)** - Stanford University, Palo Alto, CA, USA in Cooperation with the International Association for Cryptologic Research and the IEEE Technical Committee on Security and Privacy (21- 22 July 2005)

   This paper provided an overview of the various laws relevant to the problem of spam, and compared United States and European Union anti-spam legislation. It examined the extent to which law addresses the problem of spam and discussed some weaknesses. Unsolicited Commercial Communication - also known as spam - has traditionally been the most visible e-mail threat and has reached a point where it creates a major problem for the development of e-commerce and the information society. It is currently estimated that 60 per cent of all e-mail messages are spam. The United States, Australia, Canada, European Union including the United Kingdom have all recently implemented legislation in an attempt to combat Unsolicited Commercial Communication (UCE). However due to the difficulty and complexity of the problem the implementation and enforcement of the law in a global environment is still to be resolved.

5. Evangelos Moustakas, C. Ranganathan, Penny Duquenoy (2005) 'Phish or Treat? Phishing tricks reloaded' **4th European Conference on Information Warfare and Security (ECIW)** University of Glamorgan, UK (11-12 July 2005)

   The use of unsolicited e-mail communications (spam) to carry out criminal activities represents a major security threat. This paper investigated the relatively new use of spam known as 'phishing' – a form of electronic identity theft that is not only financially and personally damaging, but through loss of consumer confidence a serious threat to commercial transactions. The tricks used by 'phishers' are exposed, and an analysis of stakeholders is presented. Finally we suggested measures to counteract the threat to consumer safety and business success.

6. Evangelos Moustakas, C. Ranganathan, Penny Duquenoy (2005) 'Commercial E-mail (spam): An Exploratory Understanding Using Stakeholder Analysis' **13th European Conference on Information Systems.** Information Systems in a Rapidly Changing Economy Regensburg, Germany - [http://www.ecis2005.de] (May 23 - 25, 2005)

The growth in the use of e-mail marketing has been accompanied by an enormous increase in the amount of Unsolicited Commercial E-mail (UCE), popularly known as spam. The unprecedented amount of unsolicited messages is now recognised as a serious problem, costing the society billions of dollars very year. In this paper, we provided an exploratory understanding and conceptualisation of unsolicited commercial e-mail. Based on critical characteristics of UCE, we proposed a conceptual typology of spam. Further, we identified the key stakeholders in the UCE process and enunciated the roles played by them. Using the stakeholder analysis, we highlighted some key mechanisms for addressing the problem of UCE.

7. Evangelos Moustakas, Penny Duquenoy (2004) 'Unsolicited Commercial Communication: The integrated scenario' **ETHICOMP 2004 – "Challenges for the Citizen of the Information Society"** University of the Aegean Syros, Greece (14 - 16 April 2004)

   The growth of e-mail marketing (known as spam) is now becoming a real problem to users, causing not only financial costs, but also costs in terms of time and system integrity. These costs have been recognised and addressed by legislation in some countries. However, legislation has had little impact in part due to the territorial nature of jurisdiction. Another approach to tackling spam is to use technical measures (software applications). Although this approach goes someway to address the problem, it is not totally effective, and also raises other issues. This was the focus of this paper.

   The paper set out the extent of the problem and its impact on information society citizens, in terms of costs and risks. It then looked at some of the technical measures that are available to combat the problem, and provided an evaluation of some common applications. Finally it assessed the effectiveness of technical measures brought by Internet Service Providers and anti-spam Companies,. and concluded that technical means alone will not alleviate the problem.

   The approach of deploying a combination of $1^{st}/2^{nd}$-generation measures on the gateway servers is the best practice. Furthermore, it was suggested that despite the fact for the last 2 years the performance of various technical anti-spam solutions has been improved and the rate of false positives has been decreased a technical solution by itself is not enough to tackle the problem of spam. Users may be misled in two ways – first, that a software application will resolve the problem, and secondly, that spam is a "fact of Information society life" and their own responsibility to resolve. The co-operation between anti-spam Developers, legislation, Marketing and ISP (Internet Service Provider) Associations is the most effective way to combat and manage spam.

8. Evangelos Moustakas, Penny Duquenoy (2003) 'Service Provider Responsibility for Unsolicited Commercial Communication (spam)' **IFIP Conference on Risks and Challenges of the Network Society** Karlstad University, Sweden [http://www.cs.kau.se/IFIP-summerschool] (4 - 8 August 2003)

The focus of this paper was on the role of Internet Service Providers (ISP's) as the principle gate-keepers between the internet and e-mail-users. Legislation recognises this role and addresses the problem of spam. Other approaches to tackle the problem come from self-regulation and software applications (filtering technologies). This paper outlined some preliminary research that assesses the potential of eliminating illegal spam whilst at the same time allowing companies to use e-mail as a marketing tool, based on cooperation between the Law and the IT Sciences.

# APPENDIX D SPAM WORKSHOPS AND CONFERENCES

1. Inbox – Outbox Conference 2006 Organised by Revolution Events, ExCeL, London [http://www.inbox-outbox.com] (21-22 June 2006)

2. Internet World Conference 2006 Tracks related to: Content Management, Security, Accessibility, best practice for Web Design, Hosting, e-Commerce, e-Business [http://www.internetworld.co.uk] (9-11 May 2006)

3. 'Spam Enforcement Workshop' London Action Plan – The EU Contact Network of Spam Authorities (CNSA) (3 & 4 November 2005)

4. British Computer Society (BCS) North London Branch meeting Title: Internet Use and Abuse spam, scams, cams, clicks, blogs and more - the weird world of www today [http://www.nlondon.bcs.org] (14th September, 2005)

5. 4th ASEM Conference on eCommerce Seminar themes for the conference: Paperless Trading, Tackling spam, eLogistics, eLearning, eHealth http://www.asemec-london.org (20-22 February, 2005)

6. Conference-Exchibition 'eSecurity Uncovered 2005' http://www.esu.gsec.co.uk Williams F1 Conference Centre (25th & 26th January 2005)

7. Phishing Conference - OUT-LAW Events The Royal Society of Edinburgh [http://www.aboutcookies.org/out-law/eventinfo.asp?eventref=23] (November 23rd, 2004)

8. Workshop on Spam which was held in the Charlemagne Building of EU in Brussels (November 15th, 2004)

9. VB2004 Conference - 14th Virus Bulletin International Conference Fairmont Chicago, Illinois, USA (29th September - 1st October 2004)

10. E-mail Marketing Conference - Chicago (USA) [http://emailuniverse.com/list-news/?id=996] (September 21st, 2004)

11. EEMA Conference 'Spam the Death of e-mail?' in Dublin (Ireland) [http://www.eema.org/spamconference/programme.asp] (3-4 December 2003)

12. Workshop on Unsolicited Commercial Communication or Spam which was held in the Charlemagne Building of European Union in Brussels (October 16th, 2003)

13. Seminar Titled 'Filtering Spam: New Perspectives on the False Positive False Negative Trade-off' at Business School Oxford (June 18th, 2003)

# APPENDIX E PRESENTATIONS

- Presentation at the Marketing Research Group of Business School Middlesex University (April 27th, 2006)
- Presentation at the Polytechnic Institute of Viseu (Portugal) http://www.ipv.pt/guide/default.htm (February 28th, 2005)
- Presentation at the University of Illinois in Chicago (USA) College of Business Administration (November 8th, 2004)
- Guest Lecture at Loyola University of Chicago (USA) Loyola Marketing Club - Lewis Towers Ballroom Title: 'Unsolicited Commercial Communication (spam Tale) Problems and Possible Solutions (October 21st, 2004)
- Guest Lecture at Loyola University of Chicago (USA) Graduate Internet Marketing Class Title: 'Spam, International Dimensions and Marketing Implications' (October 27th, 2004)
- Guest Lecture at Turku University (Finland) Department of Information Technology Title: Kill Spam Volume 4 - The Integrated Scenario
- Guest lecture at Middlesex University (England) on Mobile Security (November 13th, 2003)

# APPENDIX F LIST OF ANNOTATIONS

**Association for Information Systems**
http://aisel.isworld.org/article_by_author.asp?Author_ID=6346

**Chinese Government**
Advisory Committee for State Informatisation (ACSI)
http://www.acsi.gov.cn/WebSite/ACSI/UpFile/2006/20062279 3311250.pdf

**London School of Economics**
Department of Information Systems
http://csrc.lse.ac.uk/asp/aspecis/20050023.pdf

**Nanyang Technological University, Singapore**
http://www.ntu.edu.sg/ publicportal

**Pennsylvania State University**
http://citeseer.ist.psu.edu/734427.html

**Spam Politik**
Spam Enforcement Agency in Germany
http://www.spampolitik.de/?m=20050623

**Terkko University of Helsinki**
FiNnish National Library of Health Sciences
http://www.terkko.helsinki.fi/mobile/feednavigator/?articleid=249106&j=1266&abc=i

**Universität Trier, Germany**
Department of Computer Science and Business Information Systems
http://www.informatik.uni-trier.de/~ley/db/indices/atree/m/Moustakas:Evangelos.html

**University of Dublin**
School of Computer Science and Informatics
http://www.smi.ucd.ie/~rinat/papers/ceas05_rep.html