All Party Parliamentary Internet Group

Chairman: - ***Derek Wyatt MP***
Joint Vice Chairmen: - ***Richard Allan MP & Michael Fabricant MP***
Treasurer: - ***Brian White MP***
Group Secretary: - ***Nick Palmer MP***

"Spam":
Report of an Inquiry by the All Party Internet Group

October 2003

APIG
ALL PARTY INTERNET GROUP

“Spam”

Report of an Inquiry by the All Party Internet Group

October 2003

Introduction

1. The All Party Internet Group (APIG) exists to provide a discussion forum between new media industries and Parliamentarians for the mutual benefit of both groups. Accordingly, the group considers Internet issues as they affect society, informing current parliamentary debate through meetings, informal receptions and reports. The group is open to all Parliamentarians from both the House of Commons and the House of Lords.

2. There is currently a high level of public concern about email “spam”. There is widespread disquiet about the amount of this material, its repetitiveness and the nature of the goods and services it is advertising. Additionally, many parents are particularly worried about the material being sent to their children, especially because a significant proportion of this, entirely unsolicited, email is explicitly pornographic. We are concerned that if the “spam” issue is not addressed robustly then it may serve to discredit the Internet more generally.

3. APIG issued a Press Release (*see Appendix A*) on 13th June 2003 to announce its intention to hold an inquiry into:

> “stemming the flow of bulk unsolicited email (“spam”) to UK Internet users. The inquiry will focus upon the following: the developing legislative situation (UK, EU, US and elsewhere); technical methods that may prevent spam reaching users; social methods that may prevent problems with spam; future trends in spam; and spam’s effect on other platforms (e.g. mobile phones and other devices)”.

4. We held a very well attended “Spam Summit” on 1st July 2003 at Portcullis House, London. A keynote speech was given by Stephen Timms, the E-Commerce Minister and we were also told, by other speakers, of the nature of the problems faced and the legislative situation in Europe and the USA.

5. Written submissions to the inquiry were received from:

   ActiveState Corporation
   Adva Technologies Ltd
   Advertising Standards Authority (ASA)
   AOL (UK) Ltd
   Avecho Ltd
   Blyth Community College
   Brightmail Inc
   BSI Professional Standards Services
   Caldicot Community Website Committee

Caversham Computer Services Ltd
Citigroup Global Markets Ltd
Clearswift Ltd
Committee of Advertising Practice (CAP)
Direct-Issue Ltd
EquiP Technology & CipherTrust Inc
e-relationship marketing Ltd
ESecurity4Britain (Corporact Ltd)
European Internet Service Providers Association (EuroISPA)
The European Forum for Electronic Business (EEMA)
GF Services (UK) Ltd (goingfree.com)
Global ISP Email Identity System (GIEIS) Development Team
Hairydog Ltd
Internet Policy Agency
Internet Service Providers Association (ISPA UK)
Internet Watch Foundation (IWF)
London Internet Exchange (LINX)
MessageLabs Ltd
Microsoft Ltd
Migration Solutions (Kelsall) Ltd
National Office for the Information Economy (NOIE), Australia
Network Associates Inc
Oaksys Tech Ltd
The Open University
QinetiQ Ltd and UK Data IT
Royal Mail
Sybari Software Inc
Tumbleweed Communications UK
University & Colleges Information Systems Association (UCISA)
University of Essex
University of Huddersfield
University of Leeds
Vircom Inc

and the following individuals

Danvers Baillieu
Tim Bedding
John Collins
Brian Curd
Brian Curnow
John D
Hugh Davies
Philip Godfrey
Phillip Hallam-Baker
Damon Hart-Davis
Selby Hatch
Andrew Hill
Caron Holmes
Norman Hopkins
Anne Howes
Tim Ivorson
Steve Jarvis
Mike Johnson
Mike Kew
Robin Langton & Adam Richards
David Littleboy
David Lord
John McKenna
Maureen Martin
Joe Otten
Steve Pardoe
Andy Pepperdine
D Robinson
Dan Salmon
Juan Carlos Servat
Eric Solomon
Brian Tompsett
Stuart Udall
Domenico De Vitto
Jasper Wallace
Jay Wishner

6. The committee heard oral evidence in public from:

   Clive Gringras, Partner Olswang, Chair ISPA Legal Forum

   Mary Tait, Assistant Director, European E-commerce & Communications Privacy, Department of Trade and Industry

   Phil Jones, Assistant Commissioner, Office of the Information Commissioner

   Christopher Graham, Advertising Standards Authority

   Malcolm Hutty, Regulation Officer, London Internet Exchange

   David Kehoe, VP Marketing, MessageLabs

   Gert Veendal, European Director, Brightmail

   Alyn Hockey, VP Marketing, Clearswift

   Camille de Stempel, Director of Policy, AOL UK

   Matt Lambert, Director of Government Affairs EMEA, Microsoft Ltd

   Geoff Hutton, Director, MSN UK

   Jessica Hendrie-Liano, Chair, ISPA

   Jim Cottrell, Head of Security Management, Energis

   Jeremy Beale, Head of e-Business Group, CBI

   Charles Smith, Oaksys Tech Ltd

   Steve Linford, Director, The Spamhaus Project

7. We are grateful for all the written and oral evidence that we received and also for the expert advice and assistance afforded by our specialist advisor, Richard Clayton of the Computer Laboratory, University of Cambridge.

Structure of this report

8. This report starts by considering how "spam" came to get its name and the range of different, albeit related, definitions we were presented with. We then consider what is currently being advertised by spam and not only the world-wide statistics of its prevalence, but also the many different perceptions people have of how much spam there is and how well they are individually coping. We conclude this overview of the problem by not only considering the various global estimates of the costs of spam but also by looking at the individual experiences of those who submitted evidence to us. We found that the costs were far from being just monetary in nature.

   We then look at the legislation that is currently in place within the UK for dealing with spam and at the new Regulations that are intended to be put in place for early December in order to implement our anti-spam obligations under a recent European Directive. We then survey the mechanisms proposed to enforce these laws and comment on their effectiveness.

   Having covered the legal approach to spam we then consider the technical issues, surveying how spam is currently being sent and the various technical approaches to preventing it being sent and/or arriving at its destination.

We were presented with compelling evidence that although national initiatives on spam do have some value, the problem cannot be fully dealt with except at the international level. Since much of the spam coming into the UK is sent at the behest of Americans, we report upon the various legislative initiatives that are currently taking place in the United States, making some recommendations to the legislators there. We also consider the proposed Australian legislation, which is almost, but not entirely, similar to the European model that the UK is adopting. Finally, under this topic, we consider the various international forums where further progress might be made in tackling the spam problem.

The report finishes with a brief look at a few issues that do not neatly fit anywhere else and we then summarise the recommendations that we have made.

A glossary is provided *(in Appendix B*) for those unfamiliar with the technical terms and abbreviations that are used throughout the report.

Finally, *in Appendix C*, we provide a short annotated bibliography of relevant documents that can be consulted for further and more detailed information about the issues we discuss.

What is “spam”?

9. Email continues to be by far the most important service for Internet users. Billions of messages are transferred every day. Unfortunately, a significant proportion of this traffic is unsolicited and unwanted advertising. This is often called “spam”, the derivation being from a 1970’s “Monty Python” sketch in which a group of Vikings sat in a café and incessantly chanted “spam, spam, spam, spam..” and eventually drowned out all other conversation.

10. We found some variation in the definition of exactly what “spam” is. The majority of respondents characterised it as unsolicited bulk email, though some felt that it would only be “spam” if the message it contained was a marketing message and still others thought the term should only be applied to messages of dubious taste. In this report we will use the term as meaning any email that was not requested by its recipient and has clearly been sent out en masse.

11. Many people who sent us evidence drew our attention to the fact that almost all the spam they received had been sent from foreign based systems. Though this is clearly relevant when considering whether policies or legislation are going to be effective we do not consider that its origin has any bearing on how acceptable it might be. We agree with the Open University viewpoint that the suggestion we could learn to love UK spam if only the foreign stuff could be stopped is “simply wrong”.

12. Our attention was drawn to the existence of a legitimate bulk email industry that sent “solicited” email to people who were happy to receive it. The ISP industry was also keen to indicate that they were entirely happy to process and deliver this email and that nothing should be allowed to interfere with this genuine traffic.

13. As we shall discuss below, a distinction has been made between whether spam is addressed to an individual or to a business. In their oral evidence the Department of Trade and Industry (DTI) said that they did “not see all unsolicited commercial email as such as bad” and “there are going to be many more instances where UCE is justified in a business-to-business context than it is in a business to individual context”.

14. Direct-Issue, who operate an online forum for the institutional investment community and are extensive users of email, were also concerned that “precision targeting” of sales prospects at other companies might be caught by anti-spam legislation. They compared the effect on business-to-business marketing as being similar to barring “cold calling” of prospects on the telephone.

15. However, we have noted that this summer’s DTI consultation on implementing the “E-Privacy” Directive received a very large number of responses on “cold calling” and that the DTI’s conclusion was that businesses should be able to opt-out from these calls, though practical considerations have delayed this until at least April 2004.

16. The ISP industry made it clear in their evidence, and also in their Best Current Practice documents, that they made no distinction as to whether the destination of spam was an individual or a business. Customers would infringe their

contract with the ISP by sending any spam at all and they would not be permitted to continue to do this.

17. LINX mentioned the concept of “pink ISPs” which were tolerant of spammers and asserted that there were no such organisations within the UK. LINX also observed that besides the ethical issues there were significant practical disadvantages to being perceived to be soft on spam. Network connectivity and the ability to have email delivered was not a right, but achieved through ongoing co-operation between networks. It was “simply not good business” to permit users to send spam to anyone, whatever the short-term gain in income.

18. We conclude that British business will in practice be unable to send bulk unsolicited email through UK ISPs, whether the messages are “precision targeted” or crude carpet-bombing. **We recommend that when the DTI changes the rules on business-to-business “cold calling” they should take the opportunity to explicitly ban the sending of spam to business addresses.**

What does spam contain?

19. We received evidence from a number of companies who provide filtering services that will block incoming spam. Some of these companies collect and publish statistics on the content of spam. These figures show, for example, that over time the major categories have remained “Financial”, “Internet” and “Products”. There is rather less “Spiritual” spam than in the past and “scams” remain around one in ten of the spam that was measured.

20. Brightmail reported a distinct increase “adult” spam from April 2002 (7% of spam) to April 2003 (19%) but their more recent figures show it falling back again (in August 2003 it was 12%). MessageLabs have figures for email that actually contain “pornographic attachments” and these show huge fluctuations (two or three hundred percent) from month to month. In the light of other evidence, discussed later, that a relatively small number of spammers send the overwhelming majority of spam email, we do not find it surprising to see large variations as they turn their attention from one product to another.

21. A very small proportion of spam relates to indecent images of children. The Internet Watch Foundation (IWF) acts as a clearing-house for these reports, and after an initial investigation passes the information on to the police. They told us that advertising or linking to websites containing illegal images of children was first reported to them in early 2002. By June 2002 they were receiving about 250 reports a week, with a peak of over 700. This year (in a single week in June, just before they wrote to us) they received 435 reports of which 53% actually related to child abuse websites. 80% of these websites were found to include potentially indecent images and 14 of these sites were not previously known to them.

How much spam is there?

22. The spam filtering companies also collect data on the amount of spam they detect, which they usually express as a proportion of the total email they handle. In addition, Brightmail assesses how many distinct spam “attacks” there are,

where each “attack” promotes a particular product in a particular way and may last from a few hours up to several weeks in duration.

23. Everyone agreed that the amount of spam was considerably higher now than in the past. Brightmail’s figures for individual spam attacks showed a 900% increase from April 2001 (658,579) to April 2003 (7,018,625) though much of this increase was in the first half of 2002 so that the increase from April 2002 (4,339,799 attacks) to April 2003 was “just” 62%.

24. There was also consensus between the companies that about half the overall email volume was spam (viz. that there are about 10 billion spam emails sent per day). However, there is a considerable variation between business sectors and between different parts of the world. A European company in the building trades might expect to see just 5% spam, whereas American companies in the Sports and Entertainment sector receive 78% spam on average.

25. AOL report that they are, on average, blocking 2 billion spam emails every day. Since they have approximately 26 million customers world-wide, that is an average of over 75 emails per customer.

26. The individuals and small businesses who sent us evidence reported very variable experiences of spam, though they all believed that the level that they were currently receiving was unacceptable. For example:

- Anne Howes: 20 spam emails per week;
- Damon Hart-Davis: receives 10 useful emails a day, another 30-100 were spam even after a filtering program had been used;
- David Lord: receives an average of 37 spam emails a day;
- Hugh Davies: 550 emails a day, only 5% of which is genuine email;
- Iain Harrison’s website design company: 200-300 spams per day;
- And our special advisor Richard Clayton is receiving about 9000 spam emails a day, all but 450 of which, fortunately, he is able to trivially filter.

27. UK universities are also being considerably affected. One told us that they blocked almost a third of all incoming email as clearly being spam and almost 40% of the rest was highly likely to be spam as well.

How much does spam cost?

28. Because the transfer of email is now so rapid and hence cheap, the actual “bandwidth” costs are seldom significant, even for individuals. However, our attention was drawn to people who accessed email over new generation mobile phones and here the cost of connectivity did matter.

29. Most attention on the cost of spam has related to the effort required to sort through incoming email to discard the unwanted material and locate the email that was actually required. We were told of various studies that have attempted to determine the cost of spam in terms of lost productivity to businesses (it being difficult to ascribe a monetary cost to an individual’s time in their homes).

- **Ferris Research**, January 2003

  Estimated total cost for spam in corporations in 2002 was $8.9 billion and in 2003 lost productivity costs will be approximately $14 per user per month causing the total cost to rise above $10 billion.

- **Radicati Group**, July 2003

  A company of 10,000 users with no anti-spam solution will spend on average $49 per year per mailbox in processing spam messages.

- **Vircom Ltd**, June 2003

  Lost productivity will cost a company of 1,000 users with no anti-spam solution approximately $205,000 per year.

- **MessageLabs Ltd**, June 2003

  Based on productivity loss, spam costs UK business £3.2 billion annually.

- **a UK University**, June 2003

  The direct costs of their spam-filtering system were £78,000. However, it is still costing them an estimated £1.1 million per annum, assuming that staff can deal with the spam that gets through the filters in a mere two minutes each per day.

- **Charles Smith, Oaksys Tech Ltd**

  Charles Smith came and gave us oral evidence from the point of view of an ordinary small-business email user. He told us that he receives about 1000 spam emails a day. He has built up about 280 rules within his email software which traps most of the spam. About 10 spam emails get through and he deals with these manually. He also needs to check the email that is filtered, recently he had almost missed a share trading opportunity worth £1500. He estimated that in total he spent about 20 minutes a day dealing with spam and that at his professional hourly rate this was costing him £50 a day.

30. There are many other monetary costs associated with spam. In a widely cited June 1999 report, the Gartner Group pointed out that the response of many customers to spam was to abandon their email address and change ISP. They estimated that cost of this “churn” was about $7 million annually for an ISP with a million customers. The IWF also suggested that spam was generating a general loss of confidence in the Internet.

31. However, many costs are not monetary at all. The EEMA pointed out that nobody was interested in creating an email address directory (a “white pages” service) because no names would be submitted through fear of receiving more spam. They also drew our attention to the cost of archiving spam because it was mixed in with other email that had to be preserved for business reasons. Other people pointed out the cost to entirely properly run email marketing operations when their “opt-in” messages were blocked along with the spam. A great deal of spam is forged to appear to come from legitimate businesses with consequent damage to their reputations. Our attention was also drawn to the damage to national reputations when entire towns, states or countries become inextricably linked with spam in people’s minds.

The law relating to spam

32. Where spammers make unauthorised use of third party machines or distribute viruses or “trojans” that compromise the security of a user machine, then they will almost certainly be infringing the Computer Misuse Act 1990. Clive Gringras, chair of ISPA’s Legal Forum, drew our attention to the possibility of extraditing people for offences under this Act.

33. Roland Perry from the Internet Policy Agency provided us with a detailed analysis of the law applying to the sending of “spam” within the UK. Besides the legislative provisions set out below, he also pointed out that there would be a number of generic legal issues relating to the content of spam such as the advertising or sale of prohibited products or the use of pyramid marketing.

34. The sending of bulk unsolicited email in Europe is governed by the provisions of the Data Protection Directive (95/46/EC), transposed into UK law as the Data Protection Act 1998 (DPA). This is because email addresses are “personal data” and therefore the provisions of the DPA apply. The Office of the Information Commissioner confirmed this in their 1998 Legal Guidance para 2.3.3:

> “In the context of the Internet, many e-mail addresses are personal data where the e-mail address clearly identifies a particular individual.”

35. Further analysis is provided in Opinion 1/2000 of the Article 29 Data Protection Working Party, in particular:

> Where email addresses are collected directly from a person, they must be informed of the purposes at the time of collection (Article10);
>
> The data subject must be allowed to object at the time of collection, of subsequent use, or when the list is resold (Article 14);
>
> Where the email address is collected from a public space (e.g. website or usenet) on the Internet, it is unfair processing (Article 6(1)(a)), contrary to the purpose principle (Article 6(1)(b)), and does not satisfy the balance of interest test (Article 7(f)).

36. Spam is covered by the provisions of Article 10 of the Distance Selling Directive (97/7/EC):

> “individual communications may be used only where there is no clear objection from the consumer”.

This article was not transposed into the UK’s Consumer Protection (Distance Selling) Regulations 2000 as it was felt that the combination of the Data Protection Act 1998 and Industry “self-regulation” were already providing a sufficient safeguard.

37. Additionally, most unsolicited email sent within the UK, even that which is sent by organisations which otherwise regard themselves as acting within the law, fails to abide by Article 7 of the Electronic Commerce Directive (2000/31/EC), transposed as the Electronic Commerce (EC Directive) Regulations 2002:

> Any unsolicited commercial communication must be “identifiable clearly and unambiguously as soon as it is received”.

For example, an email could meet these requirements by the presence of an ADV: prefix on its subject line.

38. In 1999 the European Union commenced a review of the whole communications framework, with the aim of condensing twelve existing Directives, developed over many years, into a consistent set of six. One of these six related to ‘data protection’ issues and became known as the Directive on Privacy and Electronic Communications (2002/58/EC). The scheme it contains for regulating spam to “natural persons” is widely described as “soft opt-in”. It is an “opt-in” (explicit prior permission) system with a “soft” exemption for existing commercial relationships, within which unsolicited email may be sent, provided that each email offers a chance to “opt-out” (refusing future contact).

39. The Directive only mandates the “soft opt-in” scheme for “natural persons” which in UK Law means not only individuals in their private capacity, but also sole traders and partnerships (but not limited liability partnerships and not any partnership in Scotland!). The Directive does not explicitly protect other legal entities, such as companies, but their “legitimate interests” must be “sufficiently protected”.

40. The new Directive is to be transposed into UK Law as the Privacy and Electronic Communications (EC Directive) Regulations 2003. A DTI consultation on these Regulations had closed shortly before we started our inquiry and the final form of the Regulations was published prior to our report. The “soft opt-in” scheme for individuals that is required by the Directive is to be introduced from the 11th December 2003, but the DTI have not imposed any new restrictions on unsolicited email to companies.

41. The final Regulations say:

> a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.
>
> with the exception that:
>
> A person may send or instigate the sending of electronic mail for the purposes of direct marketing where —
>
> (a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;
>
> (b) the direct marketing is in respect of that person’s similar products and services only; and
>
> (c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

42. As we have already discussed above, at point #18, we believe that the DTI has made a very serious mistake in not prohibiting unsolicited business-to-business email. We accept that UK based ISPs form contracts with their customers that ban all unsolicited email, whether to businesses and individuals. However, we

do not believe that ISPs should be placed in the invidious position of apparently extending the law, even though we agree that this is entirely the right thing for them to be doing. We believe that this can only lead to misunderstandings and arguments between ISPs and their customers and this will not be in anyone’s interests. **We reiterate our earlier recommendation that, when the DTI changes the rules on business-to-business “cold calling” they should take the opportunity to explicitly ban the sending of spam to business addresses.**

43. There is a further wrinkle to the distinction between sending spam to “individual subscribers” and sending it to businesses. Roland Perry pointed out that an invitation to buy Viagra sent to the sales address of a shipping company could only be construed as being sent to an individual since it would not be of any business relevance.

44. The Information Commissioner is to produce “Guidance Notes” on the new Regulations and we believe that Roland Perry’s point should be explicitly addressed therein. Therefore **we recommend that the Information Commissioner set out clear guidance as to how business-to-business communications are to be distinguished from messages intended for individual subscribers.**

45. The Committee of Advertising Practice (CAP) has updated the rules on email marketing in the British Code of Advertising, Sales Promotion and Direct Marketing (the CAP Code). The CAP Code is the rulebook used by the Advertising Standards Authority (ASA). The new rules are entirely in line with the new Privacy and Electronic Communications Regulations. The Code also requires that commercial email must make clear its nature in the subject box so recipients can delete it without opening it. This is in line with the Electronic Commerce Directive Regulations.

Enforcement of legislation

46. Under the new Regulations (and the older ones as well) it is possible for individuals or ISPs to bring an action for damages in relation to the various regulations regarding spam. Clive Gringras pointed out that a single individual would be unlikely to show that they had suffered substantial losses as the result of spam. However, groups of individuals, or ISPs on their behalf might be in a better position to be able to show the true level of damage that been incurred. He suggested that “super complaints” should be permitted, such as those that can be made by consumer organisations to the Office of Fair Trading under the Enterprise Act 2002.

47. The Privacy and Electronic Communications Regulations also provide for the Information Commissioner to deal with infringements by issuing enforcement notices. A breach of these notices can lead to court action and fines, limited to a maximum of £5000 in a magistrates court, but unlimited after a jury trial.

48. Phil Jones, an Assistant Commissioner, told us that the experience of the Information Commissioner’s Office in enforcing fax marketing rules was that they only had the resources to pursue the largest, most wilful, marketers who broke the rules.

49. The ASA told us that they were already "ahead of the game" in issuing their new rulebook. Although they had limited enforcement powers themselves, they believed in a "joined up" approach and were in a position to refer complaints on to other bodies such as the Office of Fair Trading or Trading Standards. Their view was that even where advertisements were coming from overseas, there was often a part of the business within the UK that they could go after, even if it was only a "fulfilment house". In really difficult cases they had resorted to "naming and shaming" and told us of their experience that negative publicity on morning television was effective at putting foreign advertisers out of business.

50. The ASA also told us that they had limited resources and certainly did not want to receive a copy of every spam email that was received.

51. Some evidence was submitted to us relating to the experiences some individuals had in making complaints to the ASA. It was clear from the disappointment expressed that the ASA were not currently seen to be effective in tackling spam that was sent by UK companies. However, they are clearly still learning what actions may be available to them, and a recent decision regarding an alleged "opt-in" list of email addresses has very significant ramifications in ensuring that legitimate businesses will take great care when using such lists.

> The Authority acknowledged that the advertisers had bought a list of e-mail addresses of people who had opted to receive information about business development topics by e-mail in good faith. The Authority nevertheless considered that it was the advertisers' responsibility to ensure that recipients on the list had given their explicit consent to receive such e-mails. The Authority considered that the advertisers had not got explicit consent to send the e-mail to the complainant. The Authority advised the advertisers to take more care in their targeting of marketing e-mails in the future.
>
> ASA Adjudication, "The Training Guild", 10 Sep 2003

52. Industry also told what they have been doing in the legal arena beyond enforcing their contracts with their own customers. In the USA, AOL have taken more than 100 legal actions against spammers and have won injunctions and substantial damages when these have been breached. More recently, Microsoft, Yahoo and AOL have formed an anti-spam coalition and have taken further legal action against spammers, including one UK based person.

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

54. We do not believe that the Information Commissioner has been provided with sufficient resources to be able to tackle more than a small part of the problem. **We recommend that the DTI urgently make sufficient budget available as soon as the new law is in place so that effective action can immediately be**

taken against a sufficiently large number of transgressors that this will serve to discourage any others who might be tempted to emulate them.

55. We also believe that there will always be a role for "private enterprise" enforcement actions. However, we fully accept the points made to us by Clive Gringras that individuals will often have some difficulty showing that they have suffered substantial damages through action of spammers, whereas when they were considered as a group the damage would be clear-cut. **We recommend that the DTI bring in a mechanism for "super complaints" whereby organisations acting on behalf of email users would be able to ensure that spammers could be brought to account before the courts.**

56. We note that ISPs are in a position to know how much spam of particular types is being delivered to their customers. This would be extremely relevant information when considering the appropriateness of "super complaints" and indeed in determining the level of damages that should be awarded. **We recommend that the ISP industry develop mechanisms for the release of statistical information that would be useful in the context of assessing the level of damage that is being done by particular spammers.**

57. **Since a great deal of spam is inherently illegal in what it advertises, we further recommend that other bodies such as Trading Standards and the police should give greater priority and a bigger share of their budget to pursuing any spammers that are within their reach. We also recommend that the authorities tasked with dealing with Internet crime set up formal liaison arrangements to ensure that they pass on reports of criminal activity to the appropriate authority.** It is unclear to us exactly who would investigate particular types of spam and we do not feel it should be for the public to unpick exactly where the boundaries lie when deciding where to submit reports of criminal activity.

How spam is sent

58. We were provided with a number of potted histories of the spam business. In the early days spam was mainly sent from throwaway dialup accounts. When ISPs detected the outgoing email they would shut down these accounts. To avoid this type of detection the spammers then started using other mail servers because, in those days, they were often configured to relay email for anyone who asked. As these "open relays" were secured, so that only authorised use was permitted, the spammers turned to sending their email via insecure customer machines that could be persuaded provide relay or proxy services. More recently still, some spammers have started distributing viruses whose aim is to have customer machines run hidden relaying software. Others have started to perform "brute force" searches looking for insecure passwords within otherwise secure customer email software.

59. The general picture is that nowadays about half of all the spam that is sent will pass through an innocent customer's machine on its way to its final destination. The spammer is essentially able to masquerade as the customer and will be able to access ISP services on that basis.

60. Many customers now have a broadband connection to the Internet. The number of spam emails that can now sent through a single compromised machine is therefore substantial. One respondent told us that they connected a misconfigured Microsoft Exchange server to the Internet and in just one hour it accumulated over 120,000 unauthorised outgoing spam emails. An ISP reported that they had seen 750,000 outgoing spam emails over a 24-hour period from a single customer whose machine had been exploited by a spammer.

61. There are reported to be over 680,000 open proxies currently connected to the Internet. These are used being used by spammers to send email either directly or indirectly via the local ISP. Jim Cottrell, Head of Security Management at Energis, told us that individual spammers could control up to 100,000 machines at a time.

62. Steve Linford from Spamhaus told us of their “Register of Known Spam Operations (ROKSO)” list which documents known spam operations (spammers and spam gangs) verified to have been thrown off a minimum of three consecutive ISPs for “serious spam offences”. Spamhaus states that these are the “known, determined and professional spammers, many with criminal records for fraud and theft”. At present (early October 2003) the ROKSO list contains just 150 entries (some entries are for multiple organisation names). Spamhaus assert, and appear to be universally believed, that the operations on this list are “responsible for 90% of the spam received in North America and Europe”.

63. Spamhaus also publish a list (the “SBL”) of the machines that are under the direct control of ROKSO listed groups. These spam sources are said to account for about half of the spam that is sent, viz. that which is sent direct and not via compromised third-party machines. The SBL list generally contains between one and two million distinct IP addresses, mainly in large “/16” subnets each of which contains 65,536 consecutive addresses.

Preventing spam being sent

64. A number of the solutions that were proposed to us to solve the spam problem did not take account of the current ways in which it was being sent via innocent, badly configured, insecure, customer machines. However, since many people told us that legislation was not going to solve the problem we will briefly discuss the numerous approaches that were suggested.

65. Several people suggested that the way to stop spammers was to change the economics. If, they said, email cost one cent (or one penny or whatever) to send then the spammers would find that their minuscule acceptance rates made the operation uneconomic. No one provided any figures to support the payment rate that was suggested (that if implemented would raise about 200 million dollars per day). No one provided any analysis of how payments would be accounted for, or the likely cost of the collection mechanisms.

66. Although we sympathise with the concept that the spammers should not be getting ‘something for nothing’, we can see nothing appealing in having legitimate senders of email pay. We believe that effect would just be that the spammers were not only stealing resources, but also causing significant costs

(apparently likely to reach thousands of pounds a day) for customers whose machines are insecure.

67. In addition, Clive Gringras pointed out that at present there was no guarantee that email would reach its destination. Remote systems were perfectly entitled not to accept it. ISPs who collected money from their customers for sending email would end up in an impossible position if they had contracted to deliver the email and were then unable to do so.

68. Caldicot Community Website suggested that the spam should be made uneconomic to send by targeting it from the other direction. The idea would be to promote user education so as to ensure that spam was never responded to and products promoted by it would never be purchased. We have considerable reservations about this approach, since it would be difficult to ensure that the message remained "do not buy from spammers" rather than "do not buy anything mentioned in an email" which would risk considerable damage to legitimate email marketing schemes, run on an entirely proper basis.

69. Other respondents suggested that email should be authenticated, or proposed complex systems of permission keys for the sending of email. Once again we believe these proposals would merely make it more difficult to send legitimate email whilst not effectively addressing the problem of spammers who were hijacking end-user machines.

70. We received a number of submissions that understood that the spammers' current ability to exploit insecure machines had to be addressed. They pointed fingers at the software suppliers for creating insecure systems or systems that were hard to understand and configure correctly. Others suggested that ISPs should be made responsible for the actions of insecure customers.

71. We do not accept that ISPs have sufficient control of customer systems to make it reasonable to hold them responsible for end-user machine security. However, although we heard a lot of evidence about their alacrity in dealing with customers who were the source of spam, we heard nothing about proactive efforts to detect insecure machines before the spammers managed it. **We recommend that the ISP industry develop Best Practice procedures for proactive monitoring of the security of their customers' machines.**

72. We formed the impression that there was limited assistance available to ISP customers that would allow them to secure their own machines. This summer's high profile incidents of "worms" and virus infections demonstrate that there are still a great many people who are not aware of the elementary precautions they should be taking to ensure their machines are secure. Although the ISPs have not created this situation, we feel that they are uniquely placed to address it. **We recommend that the ISP industry take urgent steps to provide clear information to customers on how to secure their machines. Self-tests should also be provided so customers can confirm that their machines are secure. There should be prominent links leading to this information from ISP websites and portals.**

Preventing spam being received

73. Many companies submitted evidence to us explaining how their systems were able to prevent their customers from receiving spam. It is not our intention in this section to endorse any of these products, which often use several different schemes in combination, but to discuss the generic issues that arise with particular types of mechanism.

74. Various claims were made for the effectiveness of prevention systems. Some companies claimed 99+% effectiveness whilst another warned that any system operating at 99% effectiveness must surely be accompanied by a high rate of “false positives”, i.e. legitimate email being discarded along with the spam.

75. The companies promoting spam-filtering systems were at pains to stress that their product should be seen as only one part of a solution. Businesses need to formulate policies on how spam is to be handled, and these should be combined with more general email policies such as guidance on the private use of email. For example, since avoiding making email addresses public is a commonly recommended spam avoidance technique, policies are needed on when business email addresses should be used for mailing lists or supplied to websites.

Blocklists

76. The idea of a blocklist is to create a database of the sources of spam (including insecure customer machines) and to reject email that arrives from these sources. The argument runs that the incoming email is far more likely to be spam than genuine email from that particular source. Joe Otten, a Computer Consultant, suggested that in addition to this blocking action going forward, ISPs should also monitor new blocklist entries and discard any stored email that had already arrived from the now recognised spam source.

77. There are said to be over 400 such lists and the rules for adding or removing entries vary very markedly. Dr Hallam-Baker reminded us that the New Zealand courts had found that entries had been made to the ORBS blacklist because of personal disputes between the owner and the companies he was listing. In his evidence to us, Steve Linford from Spamhaus contrasted the accountability his organisation accepted for the ROKSO and SBL lists, to the extent of defending court actions in Florida, with that of SPEWS – an anonymously operated blocklist – which he described as “totally unaccountable”.

78. The impact of being listed on a blocklist as a source of spam also creates a major incentive on an organisation to prevent the spam being sent. The sites that are using the blocklist will not only fail to receive any spam, but legitimate email will also be rejected. The impact of being listed can be very significant. Huddersfield University told us of the difficulties they had when a spammer forged their identity on email that had gone nowhere near their systems. Many months later they were still encountering organisations that were continuing to block email from their domain.

79. Where email has been relayed via an insecure customer and then sent to its destination via the ISP’s outgoing email systems (often called a “smarthost”) then the ISP itself can also be placed on the blocklist. This results in a situation

where no customers at all from that ISP will be able to send email to the people using the blocklist. There have been several instances of this happening to the UK's largest ISPs.

80. Although email will have been sent from a single IP address it is common for blocklists to also list nearby addresses from the same subnet. This is sometimes done to ensure proper blocking in situations where IP addresses are dynamically allocated to dial-up customers and sometimes it is just done to put economic pressure on service hosting providers to act against a single source of spam because their other customers will be affected by the block.

81. It is clear from the evidence we heard that blocklists can be extremely effective in reducing the level of incoming spam. Caversham claimed that this method alone would eliminate 90% of it and Spamhaus, as already discussed, assert that 50% of the spam is eliminated by using their list alone. However, it also quite clear to us that blocklists that are not operated in a careful manner can do considerably more harm than good.

82. We suggested to LINX that the UK ISP industry should operate a common blocklist but they told us that though they had a history of stepping forward to support initiatives when no-one else was doing so, there were already blocklists in existence so their resources were not needed. Spamhaus suggested to us that there would be a role for government recommendations of blocklists that met suitable criteria for accuracy and accountability.

83. We agree that there is a role for blocklists to play in the filtering services offered by ISPs and hence there is a need for blocklists that are operated in a fair, accurate and accountable manner. **We recommend that the ISP industry should take the lead in documenting Best Practice procedures for publishing blocklists and for using such lists to filter email. We recommend ensuring that ISPs and their customers will be able to determine whether blocklists meet the Best Practice criteria, perhaps by means of an accreditation scheme. Because blocklists can be so powerful, we recommend that careful attention be paid to mechanisms that will permit the rapid resolution of disputes.**

84. We see an important role for the DTI in endorsing industry's efforts and, by extension, endorsing organisations that run first-class blocklists. A number of public sector bodies in the UK and USA already use blocklists as part of their email filtering solution and this will undoubtedly grow, at least in the short term. **We recommend that the DTI consider the best method of ensuring that they are able to show their full and formal support for properly operated blocklists. We recommend that the DTI review how they might commit some public funds to support those blocklists that meet the highest standards and hence those that they would wish to see used by the public sector.**

Content Filtering

85. The idea of content filtering is to scan incoming email and determine whether it is spam by the application of a complex set of rules looking for emails that cross a threshold of "spamminess". Many amusing anecdotes circulate about emails mentioning Scunthorpe, or how emails to one's doctor about a Viagra

prescription might be blocked. Indeed, the introduction of a filtering system at the Houses of Parliament in early 2003 was accompanied by press stories of how it was blocking discussions of the Sexual Offences Bill and email written in Welsh! However we were assured that systems could now be very sophisticated and well able to make the correct decision as to what was or was not spam. For example, Microsoft told us they interviewed 100,000 MSN customers a year so as to determine from their customers what they felt was actually spam.

86. Many individuals drew our attention to so-called “Bayesian” filtering systems that can be trained to distinguish between spam and not-spam for an individual. Any system run by the end-user has an obvious advantage of customisation over a centralised system provided by an ISP or a third party. However a centralised system is likely to be easier to operate for someone who is less interested in ‘bells and whistles’.

87. LINX pointed out that spammers were now starting to pay attention to filtering systems and told us that we might expect spam to “evolve” over time to become more like ordinary email and thereby evade the filtering. They suggested that there was considerable advantage to be found in a diversity of solutions and from a technical point of view nothing should be done to restrict there being as wide a range as possible of potential solutions.

88. When an ISP filters email and through a “false positive” discards legitimate email by incorrectly concluding that it is spam then the customer is clearly going to be aggrieved. The ISPs try to avoid legal action for false positives by excluding liability in their contract with their customers. We consider this to be a realistic approach whilst customers have the ability to move to another ISP that filters differently or perhaps not at all. However, if the market changes in such a way that customers are likely to encounter false positives at every ISP, then it would be necessary to consider the reasonableness of ISPs avoiding responsibility for their errors by contractual means.

89. It was clear from the evidence we received that content filtering was currently believed to be an effective anti-spam approach. However, it was not always clear what sort of filtering ISPs were making available or how it might be enabled. We accept the argument that the market should decide what sort of filtering ISPs provide, if indeed any at all. However, we believe that without accurate information on what ISPs are doing, the market will not work correctly and customers will not be able to make an informed choice as to which service they should use.

90. **We recommend that ISPA should insist that its ISP members provide clear guidance to existing and potential customers as to what extent email filtering is made available and what risks this may or may not pose to legitimate email.**

Configuration checking

91. Some people suggested that spammers were “lazy” and did not ensure that their spam was fully compliant with email standards. Others pointed out how spammers will borrow legitimate identities in the hope of making their material more likely to be opened or read. The suggestion was made to us that if ISPs were more rigorous in checking that everything “matched up”, and we were

provided with extensive checklists of how this might be done, then this could be used to prevent a lot of spam arriving.

92. We do not agree with these suggestions. Many users struggle to set up their software absolutely correctly or they use laptops and then move from place to place so that although everything may “match up” in one location the settings will be wrong elsewhere. We note that email has become a remarkably successful way of communicating because systems have always been very tolerant of technical breaches of the rules. Without that tolerance the systems would be very “brittle” and sending email would be a great deal more difficult than it is today.

Advice to customers

93. There are many things that end-users can do to reduce how much spam they receive. The ASA provided with a copy of their advice leaflet *“Canning Spam”*, and we were told that ISPA and many individual ISPs have similar information on their websites.

94. A common piece of advice was to never respond to spam and in particular never to accept the invitation to opt-out of further email. The consensus was that some spammers collected the addresses of people who opted-out as being especially valuable because the addresses were valid and reached people who actually read the incoming messages.

95. This advice is clearly at odds with the position under the new Regulations that allow companies to send unsolicited email to existing customers until they ask to opt out – precisely what the recipients have previously been told that they should not be doing!

96. We note that the Information Commissioner is proposing to tackle the general need for advice by recommending particular websites as being accurate and accessible. Within this general advice, there is an obvious need for a source of authoritative guidance as to when opt-out instructions within an unsolicited email should or should not be followed.

97. **We recommend that the DTI accept that it has a special role to play in user education and it should be providing authoritative advice on opt-out provisions. We also recommend that ISPA and the ISP industry as a whole should review their existing advice to ensure that the legitimacy of some opt-out provisions is properly recognised.**

International considerations: USA

98. Many respondents pointed out that a new generation of laws in Europe would not make much practical difference to how much spam was received because spam was an international problem. Particular attention was drawn to the situation in the United States where there was no federal law on spam.

99. Thirty-five US states have laws relating to spam, though provisions vary considerably. A number of common ideas can be seen, notably specific labelling requirements (marking of email by ADV or ADV:ADLT) and the requirement that subject lines should not be misleading. Many states have requirements to correctly identify the source of the email, prohibitions on misleading routing information and penalties for hiding the sender’s identity or appropriating the identity of a third party. There is often a requirement to include “opt-out” instructions within the email and penalties for failing to honour these opt-outs.

100. We were told that the laws had been singularly ineffective in preventing spam with the spammers routinely ignoring their requirements. Although there were some exceptions, the laws were often being used just to prosecute legitimate companies who had made a technical error in compliance.

101. There have been several attempts at creating a federal law, but those Bills that had emerged from the House of Representatives or the Senate had failed at the next, joint committee, stage that attempts to unify the wording of disparate proposals. There are currently several Bills being considered by Congress, and we were briefed on which were most likely to make any progress.

102. Because the consensus is that whatever law is finally passed in the USA will be of global significance, we consider it appropriate to comment upon the various components that it may or may not contain.

Labelling

103. We see nothing contentious in the notion that bulk email should not mislead as to its content or origin. We have already remarked upon the damage that can be done to innocent third parties when email is sent out in their name, and we cannot see that businesses or consumers are served in any way by email that does not immediately disclose its true source.

104. We also see immense value in rules that prohibit misleading Subject lines so that the recipient is fooled into opening messages that they would have ignored apart from the deception. Although we can see the attraction of fixed format labelling such as ADV, we are concerned that unless universal rules are adopted the existence of contradictory requirements in different jurisdictions will merely make things more difficult for people sending permission-based email.

105. We note that accurate labelling and provenance means that people who wish to deploy filters will be able to do this with confidence that email will not “sneak past them”. This will mean that such filters will not need continuous tweaking and will therefore reduce the costs of those who choose to employ them.

Opt-out, opt-in and very soft opt-in

106. We were told that, at present, Congress is most likely to pass an “opt-out” style law that would require unsolicited bulk email to include instructions for removal. There would be no requirement for recipients of email to have given their permission for the email to have been sent.

107. We were also told, most colourfully by Steve Linford from SpamHaus, but by others as well, that the effect of such a law would be to legitimise existing senders of spam. The existing controls, weak as they were, would become ineffective and we could look forward to substantially more material arriving than at present.

108. Our attention was drawn to the existence of in excess of 23 million small businesses in the United States, with a turnover of about 1 million per year. If just 1% of these businesses sent an unsolicited email to an individual, then that individual would be opting-out of future mailings once every two minutes, 24 hours a day for the next year. This would clearly be unacceptable.

109. One of the Bills introduced in the Senate would create a “do not email” list run by the FTC, rather like the “do not call” telephone preference service that the Americans have recently implemented. Since there are no firm plans to comment upon, it is possible to be over-critical, but we would be particularly concerned that such a plan might be for Americans only, whereas domains such as “.com” are international in scope and so there is a recipe here for immense confusion. We fear that such a scheme would not assist individuals and businesses in the UK at all.

110. California’s legislature has now passed a Bill (SB186) that enacts an “opt-in” permission-based scheme. However, the “soft” proposal within this that allows businesses to email their existing customers is distinctly weaker than the scheme within the European Directive. Businesses would be able to lawfully send emails on behalf of other businesses or to promote very different products or services than the one that formed the original relationship. This still gives considerable scope for the sending of junk email by ISPs, portals and indeed conglomerates. Unsolicited political email is also unaffected.

Other proposals

111. There are some interesting sub-components of a federal law that are being floated as ideas. Of particular note is the proposal that persistent spamming should become equated with “racketeering” so that the provisions of RICO could be applied. The argument runs that many of the spammers identified by lists, such as SpamHaus’s ROKSO list, are career criminals who have merely turned to the sending of spam as a well-paid alternative to other illegal actions.

112. Also of interest is the notion being promoted by some pressure groups that the Department of Justice should be empowered to place a reporting requirement upon anyone convicted of spamming. This would require them to keep records of further emails that they send. Further spamming would therefore be easily detected and if the records were falsified this would, of itself, be treated as a serious offence.

113. Some of the Bills before Congress also bring in penalties for “hacking” style offences such as unauthorised use of third-party machines, “dictionary” attacks that attempt to find valid email addresses by brute force and “address harvesting” of addresses from websites and other locations. The UK Regulations have not needed to address these issues because they were already covered by the Computer Misuse Act 1990, or by general provisions within the Data Protection Act 1998.

Pre-emption

114. Since the existing state laws have significant differences, there is a considerable lobby for a federal law to explicitly over-ride these existing statutes. This will simplify things for the senders of unsolicited email because their actions will not be lawful for recipients in some states but not in others. As California, and perhaps other states, adopt “opt-in” proposals then a federal “opt-out” scheme would be immensely confusing and of course those who lobbied against “opt-in” have an obvious wish to re-run the battle in Washington.

115. Unfortunately, the desire for consistency does not seem to extend to any wish for US laws to be consistent with the European Directive as being enacted in the UK and throughout the EU. This is extremely relevant because many European and British businesses use “.com” domain names and although this top level domain is intended to be “international” there is a regrettable trend for US based companies to see it as evidence of the holder being US based.

Recommendations

116. **We recommend to the US Congress that they adopt an anti-spam law that is modelled as closely as possible along the lines of the European Directive on Privacy and Electronic Communications (2002/58/EC).** As legislators ourselves we recognise that there is often a prejudice against “foreign” proposals and that “not invented here” is a powerful, if irrational, argument. However, we feel very strongly that the advantages of having a consistent set of laws between Europe and the USA (and also with Australia who are moving towards a European style scheme) would have huge advantages for everyone.

117. Many of the people who gave evidence to us believed that the hard-core of “professional” spammers who are currently resident in the USA would go “off-shore” if the USA was to make spamming illegal. Indeed some were reported to already be operating from China. However, if Europe and the USA were to have consistent laws then there would be considerable pressure on other parts of the world to also fall into line.

International considerations: Australia

118. The Australian National Office for the Information Economy (NOIE) recently produced a detailed report on the spam problem and how it can be countered. They recommended that the Australian government should bring forward legislation to prohibit commercial electronic messaging without the prior consent of the end user unless there is an existing customer-business relationship.

119. A bill has now been brought forward (“The Spam Act 2003”) which establishes a European-style “opt in” system with a similar “soft” arrangement such that commercial email may be sent to existing customers provided that the recipient has the ability to “opt out”.

120. There are, however, some differences from the European Directive. The proposed legislation does not restrict a business to only advertising its own, similar, products. It also explicitly excludes messages sent by “government bodies, registered political parties, religious organisations, and charities”.

121. We are unaware of how many charities there might be in Australia, but in the UK there are about 188,000. There will also be a fair number of government bodies, political parties and religious organisations. Although we can see the political attractiveness of exempting bodies such as charities from anti-spam legislation, we fear that this may prove to be short-sighted if a significant number of them misinterpret the legislation as meaning that spam from all of them would be in any sense acceptable to the recipients.

122. **As with the US Congress, we recommend that the Australian Parliament carefully consider the advantages – in this ever more closely connected world – of an entirely consistent anti-spam regime in every country. We recommend that they adopt rules that run as closely as possible along the lines of the European Directive on Privacy and Electronic Communications (2002/58/EC).**

Current international initiatives

123. During our oral evidence sessions we asked many witnesses to tell us about the international initiatives that were taking place. We were uniformly disappointed with the answers that we received. The most positive suggestions came from the DTI who thought that it was on the agenda for the OECD and perhaps the ITU.

124. An OECD initiative on cross-border fraud was published in June 2003, however this is only one part of the problem and does not address spam that advertises legitimate business products, but in a illegitimate manner.

125. In December, the ITU, in conjunction with the UN, are holding a World Summit on Information Society (WSIS). Our research indicated that spam is not explicitly on the agenda.

126. The Internet Research Task Force (IRTF), who promote research of importance to the evolution of the future Internet, has set up an “Anti-Spam Research Group” (ASRG) to look into the ways in which technical changes might be

made so as to impact the spam problem. It is to specifically avoid consideration of legal issues, but is intended to define the problems faced, consider possible solutions and to pay particular attention to the issues that arise in getting them widely deployed. It is hoped that the ASRG can develop technologies that can then be standardised within the Internet Engineering Task Force (IETF) framework, the group that creates the standards on which today's Internet works. Unfortunately, judging from the progress so far, the ASRG is not going to produce rapid results.

127. We consider that spam poses a considerable threat to the email infrastructure within the UK. We are concerned that the UK is doing so little on the general international stage to get it onto the agenda of international forums. We have a particular concern, as outlined above, that legislative developments in the USA may have a very negative impact here. **We recommend that the UK Government, acting through the DTI and the Foreign Office, take urgent steps to make British and European concerns about spam known to the US Government, US legislators and other Governments world-wide.**

128. **Given the OECD's excellent start on one part, albeit an important part, of the spam problem, we recommend that the Government press for further work within this forum with the aim of creating consistent anti-spam legislation on a world-wide basis.**

General

129. As is inevitable, some of the issues on which we received evidence, and which we agree are important, do not fit into tidy categories, nor are they specifically concerned with particular pieces of legislation. This final section of our report briefly covers these topics.

130. Dr Hallam-Baker suggested to us that reducing the level of spam might make criminal schemes more credible. One "Nigerian email" promising millions of dollars in an Advanced Fee Fraud might be plausible to some, ten a day could never be. Whilst we appreciate his point, we feel that the damage done by the current level of spam far outweighs any considerations of protecting the gullible and greedy from themselves.

131. The Open University warned us that we might expect to see widespread spam appearing on Instant Messaging systems. Although technical blocking measures to counter this would need to be technology specific, we believe legislation should have fewer problems since it is usually sufficiently generally expressed to catch any and all Internet based messaging systems. Indeed the European Directive also covers SMS text messages on mobile phones.

132. One respondent suggested that servers should be deployed that would mount "denial of service" attacks against servers that were sending spam. Besides the collateral damage done to the network on the route to the spam source, we rather suspect that this approach would be entirely illegal under international law and we cannot support it.

Summary of Recommendations

#18 **We recommend that when the DTI changes the rules on business-to-business “cold calling” they should take the opportunity to explicitly ban the sending of spam to business addresses.**

#44 **We recommend that the Information Commissioner set out clear guidance as to how business-to-business communications are to be distinguished from messages intended for individual subscribers.**

#53 **We recommend that the DTI urgently review the ability of the Information Commissioner to police the new Regulations on the sending of spam and provide appropriate powers to deal with what will inevitably be rapidly changing situations.**

#54 **We recommend that the DTI urgently make sufficient budget available as soon as the new law is in place so that effective action can immediately be taken against a sufficiently large number of transgressors that this will serve to discourage any others who might be tempted to emulate them.**

#55 **We recommend that the DTI bring in a mechanism for “super complaints” whereby organisations acting on behalf of email users would be able to ensure that spammers could be brought to account before the courts.**

#56 **We recommend that the ISP industry develop mechanisms for the release of statistical information that would be useful in the context of assessing the level of damage that is being done by particular spammers.**

#57 **Since a great deal of spam is inherently illegal in what it advertises, we further recommend that other bodies such as Trading Standards and the police should give greater priority and a bigger share of their budget to pursuing any spammers that are within their reach. We also recommend that the authorities tasked with dealing with Internet crime set up formal liaison arrangements to ensure that they pass on reports of criminal activity to the appropriate authority.**

#71 **We recommend that the ISP industry develop Best Practice procedures for proactive monitoring of the security of their customers’ machines.**

#72 **We recommend that the ISP industry take urgent steps to provide clear information to customers on how to secure their machines. Self-tests should also be provided so customers can confirm that their machines are secure. There should be prominent links leading to this information from ISP websites and portals.**

#83 **We recommend that the ISP industry should take the lead in documenting Best Practice procedures for publishing blocklists and for using such lists to filter email. We recommend ensuring that ISPs and their customers will be able to determine whether blocklists meet the Best Practice criteria, perhaps by means of an accreditation scheme. Because blocklists can be so powerful, we recommend that careful attention be paid to mechanisms that will permit the rapid resolution of disputes.**

#84 **We recommend that the DTI consider the best method of ensuring that they are able to show their full and formal support for properly operated blocklists. We recommend that the DTI review how they might commit some public funds to support those blocklists that meet the highest standards and hence those that they would wish to see used by the public sector.**

#90 **We recommend that ISPA should insist that its ISP members provide clear guidance to existing and potential customers as to what extent email filtering is made available and what risks this may or may not pose to legitimate email.**

#97 **We recommend that the DTI accept that it has a special role to play in user education and it should be providing authoritative advice on opt-out provisions. We also recommend that ISPA and the ISP industry as a whole should review their existing advice to ensure that the legitimacy of some opt-out provisions is properly recognised.**

#116 **We recommend to the US Congress that they adopt an anti-spam law that is modelled as closely as possible along the lines of the European Directive on Privacy and Electronic Communications (2002/58/EC).**

#122 **As with the US Congress, we recommend that the Australian Parliament carefully consider the advantages – in this ever more closely connected world – of an entirely consistent anti-spam regime in every country. We recommend that they adopt rules that run as closely as possible along the lines of the European Directive on Privacy and Electronic Communications (2002/58/EC).**

#127 **We recommend that the UK Government, acting through the DTI and the Foreign Office, take urgent steps to make British and European concerns about spam known to the US Government, US legislators and other Governments world-wide.**

#128 **Given the OECD’s excellent start on one part, albeit an important part, of the spam problem, we recommend that the Government press for further work within this forum with the aim of creating consistent anti-spam legislation on a world-wide basis.**

Appendix A: Press Notice & Guidelines for Witnesses

13th June 2003
For immediate release

Press Release

All Party Internet Group to hold public inquiry on “spam”

The All Party Parliamentary Internet Group (APIG) is to hold a public inquiry into stemming the flow of bulk unsolicited email (“spam”) to UK Internet users.

The inquiry will focus upon the following:

- The developing legislative situation (UK, EU, US and elsewhere);
- Technical methods that may prevent spam reaching users;
- Social methods that may prevent problems with spam;
- Future trends in spam; and
- Spam’s effect on other platforms (e.g. mobile phones and other devices)

APIG calls upon interested parties to present written evidence to the inquiry before June 25th 2003.

Public hearings will be held in the House of Commons on the 3rd and10th July when MPs will hold oral evidence sessions with industry, Government and the public.

To launch its work on spam, APIG is hosting a “Spam Summit” in Westminster on 1st July 2003. Due to limited space, attendance at the Summit will be by invitation only. For further information on the Spam Summit please email spamsummit@gbc.co.uk

Derek Wyatt MP, Joint-Chair of APIG said:

“Spam will soon be the majority of emails sent. Ultimately we will need a new global level organisation to “hold” issues about the Internet and APIG’s evidence sessions will be an opportunity to explore this area as well as look for more immediate inter-government action and technical solutions.”

Richard Allan MP, Joint-Treasurer of APIG said:

“Dealing with spam is a key issue in helping to make the Internet usable for people in the UK. It is essential that we find solutions that the industry can employ to ensure that email use is not severely affected by the continued growth in spam levels.”

Brian White MP, Joint-Treasurer of APIG said:

In order to increase user confidence in the Internet and increase take-up levels for broadband it is essential that all stakeholders work together to combat the growing of spam.”

Written evidence should be submitted to inquiry@apig.org.uk by 25th June 2003. APIG may, at its discretion, ask for oral evidence from witnesses on 3rd July and 10th July at the House of Commons. The inquiry's report is expected to be published in the autumn.

Note to Editors:

Derek Wyatt MP is the Labour MP for Sittingbourne and Sheppey. He is a leading campaigner on Internet issues in Parliament.

Richard Allan MP is the Liberal Democrat IT spokesman and represents Sheffield Hallam.

Brian White MP is a leading Labour backbencher on technology issues representing Milton Keynes North East.

The All Party Parliamentary Internet Group exists to provide a discussion forum between new media industries and parliamentarians. Accordingly, the group considers Internet issues as they affect society, informing Parliamentary debate through meetings, informal receptions, inquiries and reports. The group is open to all members of the Houses of Parliament.

Enquiries about the work of the Committee:

Telephone: 020 7233 7322

Fax: 020 7233 7294

e-mail: inquiry@apig.org.uk

APIG Inquiry: Guidelines for Witnesses

The All Party Parliamentary Internet Group announced an inquiry into “spam” on 13th June 2003. The inquiry is anxious to receive as wide a range of submissions as possible.

1. More information about APIG can be found at **http://www.apig.org.uk**
2. Recent documents of relevance to the inquiry include:
   - The Telecoms Data Protection Directive (97/66/EC)

     http://europa.eu.int/ISPO/infosco/telecompolicy/en/9766en.pdf
   - The Directive on Privacy and Electronic Communications (2002/58/EC)

     http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/ l_20120020731en00370047.pdf
   - The DTI consultation on the implementation of the Directive on Privacy and Electronic Communications

     http://www.dti.gov.uk/industry_files/word/complete_document.doc
   - The E-Commerce Directive (implementing Regulations have provisions affecting UCE)

     http://www.dti.gov.uk/industries/ecommunications/ electronic_commerce_directive_0031ec.html
3. Members of Parliament daily receive a mass of papers. If a memorandum is to command their attention, it should be brief and to the point. In particular, it should address the matters raised by the inquiry and concentrate on the issues with which

the witness has a special interest. A typical length would be about 1,000 words. Essential statistics or further details can be added as appendices.

4. It would be greatly appreciated if memoranda could be submitted electronically either in plain ASCII, Adobe PDF format or in Microsoft Word .DOC or .RTF format. Ideally, pages and paragraphs should be numbered. Memoranda should be dated, with the name, address and telephone number of the person in the organization who is responsible for submission given at the end. Memoranda should be submitted to the address at the end of this notice.
5. It is at the inquiry's discretion to print any evidence it receives. Any information that a witness would not wish to be considered for publication should be clearly marked.
6. The inquiry has asked for all written evidence to be submitted by 25th June 2003 although extensions to that deadline may be considered. The inquiry may decide, having read a memorandum, to invite a witness to give oral evidence.

Evidence may be submitted to:

APIG Secretariat,
23 Palace Street,
London
SW1E 5HW

Electronic submissions (in plain ASCII, Adobe PDF or Microsoft Word .DOC or .RTF formats) are preferred and can be emailed to inquiry@apig.org.uk

Appendix B: Glossary of Terms

ADV
label in an email subject line to show that it is an advert

AOL
a large ISP operating at a global level (originally "America Online")

APIG
All Party Internet Group: a discussion forum for Parliamentarians and the new media industries

ASA
Advertising Standards Authority: the independent self-regulatory body for non-broadcast advertisements, sales promotion and direct marketing in the UK

CAP
Committee of Advertising Practice: the self-regulatory body that creates, revises and publishes the rule book for non-broadcast advertisements, sales promotions and direct marketing in the UK

DPA
Data Protection Act 1998

DTI
Department of Trade and Industry: part of the UK Government

EEMA
the European Forum for Electronic Business

EU
European Union

FTC
Federal Trade Commission: US Government body charged with enforcing federal laws relating to trade, business and consumers.

ISP
Internet Service Provider

ISPA
Internet Service Providers Association UK: a “trade body” for the UK ISP industry

IWF
Internet Watch Foundation

IP address
unique identifier for a connection to the Internet

ITU
International Telecommunications Union

LINX
London Internet Exchange: a neutral not-for-profit partnership that operates the premier UK Internet exchange point

MSN

Microsoft's web portal

OECD

Organisation for Economic Co-operation and Development

open proxy

a proxy will allow other machines to use it to make connections to services on their behalf. An open proxy will allow any other machine to use it, whether they would normally have permission to access the service or not.

open relay

an email relay will accept email and pass it onward to its true destination. An open relay will do this on behalf of any machine on the Internet, whether there is a contractual arrangement to prevent abuse or not.

ORBS

Open Relay Behaviour-modification System: a New Zealand based organisation that operated a blocklist

RICO

Racketeering, Influence and Corrupt Organizations Act: US legislation dealing with topics such as "organised crime" [18 U.S.C. §§ 1961-1968]

ROKSO

Spamhaus's "Register Of Known Spam Operations": this documents the identity of spammers and spam gangs accused of "serious spam offences" by multiple ISPs

SBL

Spamhaus's "Spam Block List": which documents IP address ranges controlled by ROKSO listed groups

spam

email that has not been requested by its recipient and that is sent out en masse

SPEWS

Spam Prevention Early Warning System: a blocklist of known spam sources and spam friendly hosts

trojan

a "trojan horse" is a computer program that is ostensibly for one purpose but contains further code that you would never have executed if you knew its true purpose which will be to compromise the security of your system

UCE

Unsolicited Commercial Email: a subset of what we call spam

virus

a self-replicating computer program that spreads from machine to machine, usually, these days, by email. Usually distinguished from a worm by living within an identifiable file or files.

worm

a self-replicating computer program that spreads from machine to machine via network. Usually distinguished from a virus by not requiring to reside in a file or email.

Appendix C: Bibliography

European directives

The Data Protection Directive (95/46/EC)

http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf

The Distance Selling Directive (97/7/EC)

http://europa.eu.int/comm/consumers/policy/developments/dist_sell/dist01_en.pdf

The Telecoms Data Protection Directive (97/66/EC)

http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf

The Electronic Commerce Directive (2001/31/EC)

http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

The Directive on Privacy and Electronic Communications (2002/58/EC)

http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

UK legislation

Data Protection Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Consumer Protection (Distance Selling) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002334.htm

Electronic Commerce (EC Directive) Regulations 2002

http://www.hmso.gov.uk/si/si2002/20022013.htm

UK implementation of the Directive on Privacy and Electronic Communications

DTI website

http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html

DTI consultation document, March 2003

http://www.dti.gov.uk/industry_files/word/complete_document.doc

Privacy and Electronic Communications (EC Directive) Regulations 2003

http://www.hmso.gov.uk/si/si2003/20032426.htm

International legislation

US state laws

http://www.spamlaws.com/state/index.html

Proposed US federal laws

http://www.spamlaws.com/federal/index.html

Australian Spam Bill 2003

http://scaleplus.law.gov.au/html/bills/0/2003/0/2003091906.htm

… and the Australian Spam (Consequential Amendments) Bill 2003

http://scaleplus.law.gov.au/html/bills/0/2003/0/2003091905.htm

Other relevant documents

OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders

http://www.oecd.int/dataoecd/24/19/2956420.pdf

Article 29 Working Party: Opinion 1/2000 on the implementation of Directive 95/46/EC

http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp28_en.pdf

The British Code of Advertising, Sales Promotion and Direct Marketing (usually known as “the CAP code”)

http://www.asa.org.uk/the_codes/index.asp

The ASA adjudication relating to “The Training Guild”

http://www.asa.org.uk/adjudications/show_adjudication.asp?adjudication_id=36597

The Spamhaus ROKSO list

http://www.spamhaus.org/rokso/index.lasso

Charter of the Anti-spam Research Group (ASRG) of the IRTF

http://www.irtf.org/charters/asrg.html

Statement by the Hormel Foods Corporation regarding their SPAM trademark

http://www.spam.com/ci/ci_in.htm

Written and oral evidence submitted to this inquiry

http://www.apig.org.uk/spam_inquiry.htm

APIG

ALL PARTY INTERNET GROUP