Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

11-Mar-2004

English text only

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/CP/ICCP(2004)1
Unclassified

OECD WORKSHOP ON SPAM

REPORT OF THE WORKSHOP

2-3 February 2004
Brussels, Belgium

This unclassified document is a report of the OECD Workshop on Spam, held at the European Commission in Brussels, Belgium on 2-3 February 2004. It is submitted to the upcoming meetings of the Committee on Consumer Policy (18-19 March), the Working Party on Information Security and Privacy (30-31 March) and the ICCP Committee (1-2 April) for information.

This document will be posted on the OECD Web site on spam at www.oecd.org/sti/spam

Contacts: Dimitri Ypsilanti, Tel.: +33 1 45 24 94 42, dimitri.ypsilanti@oecd.org;
Anne Carblanc, Tel: +33 1 45 24 93 34, anne.carblanc@oecd.org;
Michael Donohue, Tel: +33 1 45 24 14 79, michael.donohue@oecd.org; Fax: +33 1 44 30 62 59

JT00159766

English text only

OECD WORKSHOP ON SPAM: REPORT OF THE WORKSHOP

1. The OECD held a Workshop on Spam in Brussels on 2-3 February 2004, which was hosted by the European Commission (EC) (Directorate General Information Society). The event was organised jointly by the ICCP's (Committee for Information, Computer and Communications Policy) Working Parties on Telecommunications and Information Services Policy (TISP) and Information Security and Privacy (WPISP), and the Committee on Consumer Policy (CCP). The workshop attracted some 260 participants. OECD Deputy Secretary-General Herwig Schlögl and EC Commissioner for Enterprise and the Information Society Erkki Liikanen delivered opening speeches. In addition, 54 speakers and panellists were gathered from government, industry and civil society.

2. The objective of the workshop was to explore the growing problem of spam, with a particular focus on its international dimension. Day 1 concentrated on understanding spam and its impacts. Day 2 focused on existing approaches to combating spam and possible future work in this area. Finally, participants discussed useful steps that could be taken at the international level, including by the OECD.

3. This document includes a list of main points that emerged from the workshop, followed by summaries of each of the nine sessions. It has been prepared by the Secretariat.

4. Presentations delivered at the workshop and other workshop materials are available online via the OECD Web site on its work on spam at www.oecd.org/sti/spam

Main points

5. The following key points emerged in presentations and discussions during the workshop and, in particular, reflect the main points highlighted during the last session's moderated discussion on next steps.

Spam is a growing problem requiring urgent action

6. Over the last number of years there has been a dramatic increase in levels of spam being sent. Spam imposes societal and economic costs on all categories of Internet users, network administrators and service providers. There is an urgent need for action to counteract the negative effects that spam is having on trust and confidence online, on the reliability of e-mail as a communications medium, and on the growth of the digital economy more generally.

A multi-disciplinary approach, inclusive of all stakeholders, is needed to combat spam

7. There is no single solution to the problem of spam. A multi-disciplinary approach focusing on technical, regulatory and self-regulatory measures as well as consumer and business education is necessary in order to develop sustainable solutions to spam. The success of any anti-spam strategy will depend on co-operative efforts of all stakeholders, from governments to industry to civil society organisations and individual users.

Sustainable solutions need to focus on the underlying causes and incentives of spam...

8. Most current anti-spam solutions are retroactive, focusing on the effects of spam. Long-term sustainable solutions will also need to strike at the causes and incentives for sending spam. Some have

noted that work is already underway on new authentication systems or payment mechanisms for senders of bulk e-mail. Further study is needed on the viability of these proposals.

But solutions to spam must not burden legitimate actors

9. In order to maintain the open character and financial promise of the Internet, as well as safeguard privacy, solutions to spam must avoid placing unnecessary burdens on Internet users (both individuals and businesses) or on Internet and e-mail service providers.

Spam requires a co-ordinated approach within national governments

10. Even within national governments, there may be a number of agencies with authority over spam. There is a need to co-ordinate action among these agencies and, where possible, identify a single contact point where individual users and businesses can report and seek solutions to spam.

Spam is a global problem requiring a globally co-ordinated response

11. As spam can originate in any country in the world where there is Internet access, effective international co-operation is essential to develop and implement anti-spam solutions. Possibilities for such co-operation have been suggested in several areas, including: the widespread adoption of anti-spam laws and policies to ensure that there are no safe havens for spam; development of appropriate tools for law enforcement agencies to conduct or assist with cross-border investigations and prosecutions; internationally co-ordinated best practices for key industry players (Internet and e-mail service providers) and public/private partnerships, especially in the areas of reporting, investigation and awareness-raising.

Report of the workshop

Welcome and introduction

12. **Herwig Schlögl,** Deputy Secretary-General of the OECD, opened the workshop. He extended a warm welcome to all participants and thanked the European Commission for offering to host the event.

13. Mr. Schlögl noted that, since the emergence of the Internet, one of the key challenges facing governments, business, and civil society has been how to build trust in this new medium. He recalled that the OECD had been active in this area for a number of years and had already issued guidelines in the areas of consumer and privacy protection, information security and cross-border fraud and deception.

14. He highlighted some of the problems caused by spam and noted how these had the potential to seriously undermine trust in the Internet. He discussed the varied legislative approaches taken by OECD countries to address the problem of spam. He explained how the OECD could provide a useful forum for countries to compare notes on the operation of these varied approaches in practice. Further, he noted that no single legislative solution was likely to bring an end to spam on its own and that a more comprehensive package of measures that includes technical solutions, education and awareness, self-regulation and enforcement co-operation was needed. He suggested that the wide ranging expertise of the OECD committees and its experience in bringing together all relevant policy communities meant that it was a suitable venue for developing a multi-dimensional action plan at the international level.

15. **Erkki Liikanen,** EC Commissioner for Enterprise and the Information Society, welcomed participants. He stated that the European Commission was proud to host this OECD workshop on spam, which it now considered to be one of the biggest challenges to the information society. He deduced from the high level of participation in the workshop that OECD countries shared this view. He noted that the

European Union's (EU) 2002 *Directive on privacy and electronic communications* requires opt-in consent for all electronic commercial communications to individuals; prohibits commercial messages which disguise or conceal the identity of the sender; and requires all commercial messages to include a valid return address. He outlined a series of next steps which the Commission planned to take focusing on effective implementation and enforcement of existing laws, self-regulatory and technical actions by industry, and awareness campaigns. He stated that the fact that as so much spam comes from outside EU borders it made it imperative to supplement national and regional measures within the EU area with international action. He concluded that the OECD was very well placed to play a prominent role in the fight against spam at the international level and urged it to promptly develop a concrete framework for action.

Session 1, Part 1: Understanding spam

16. The aim of this session was to provide an introductory understanding of spam and its most common characteristics. Speakers and panellists looked at the kind of spam that is being sent, where it is coming from, and some of the challenges to combating it.

17. There was a consensus among government, consumer and industry representatives that spam was having a very negative impact on consumers trust and confidence online and that if it continued, increasing numbers of consumers would turn away from online activities and e-commerce. They also expressed concern that spam was reducing confidence in e-mail as an effective and reliable communication medium.

18. As regards the content of spam, speakers agreed that a significant amount of spam involves fraudulent or deceptive messages, such as bogus get-rich-quick schemes or miracle diets. It was noted that these kinds of messages are illegal in most countries, even those that do not yet have anti-spam laws, under laws prohibiting fraudulent, unfair or misleading advertising or commercial practices.

19. A clear distinction was drawn between spam and legitimate commercial e-mail. One speaker noted that spam is untargeted and unwanted e-mail which offers recipients no valid means to opt -in or out. Legitimate commercial e-mail on the other hand respects the opt-in or opt-out rights of recipients depending on the country they operate in.

20. The point was made that it is very hard to tell where spam originates because it is easy for spammers to mask their identities and location by falsifying names and e-mail addresses in e-mail headers or by routing their messages through open proxies or relays. This makes it very difficult to track down, investigate and prosecute spammers. One speaker focused on the need to educate businesses about the problem of open proxies and mail relays so that they did not unwittingly become a source of spam. He referenced a recent initiative known as "Operation Secure your Server," conducted by the US government, acting in co-operation with 26 other consumer protection and law-enforcement agencies around the world. As part of this initiative, the government agencies sent advisory letters to operators of sites around the world that have insecure servers, explaining the problems associated with these servers and providing instructions on how to secure them.

21. There was disagreement among some of the panellists, and members of the audience, on the issue of whether an opt-in or opt-out approach should be adopted for unsolicited e-mail. Those in favour of opt-in noted that consumers overwhelmingly supported this approach; that there are so many e-mail marketers operating today that it would be unduly burdensome, if not impossible, to opt-out of all of these unwanted solicitations; and that even if a centralised opt-out list were created it could become a rich target for spammers seeking to obtain e-mail addresses. Those in favour of opt-out were primarily concerned with the costs to legitimate commercial marketers of this approach. Finally, one speaker cautioned against focusing on this matter for too long noting that the majority of spam being sent today would violate either

the opt-in or opt-out approach. He suggested that it was more important for countries to find ways to co-operate to put an end to this kind of spam rather than to engage in lengthy debate on whose national approach was best.

Session 1, Part 2: Understanding spam

22. This part of the session focused on efforts to measure spam and its rate of growth. Speakers and panellists outlined existing approaches to measuring spam and evaluated their accuracy and reliability.

23. From the outset, the point was made that the lack of a common definition of spam makes it very difficult to measure spam. It was suggested that this may account for the great disparity in figures that are circulated today. There was a consensus, however, that although there may be difficulties in calculating precisely the percentage of e-mail traffic that constitutes spam, there could be no doubt that spam was increasing and that it was approaching a stage where e-mail was becoming unusable.

24. The specific figures presented in this session were based on different methods of calculation. The first were from a large commercial provider of filtering software and were based on the e-mail being trapped in these filters. These figures estimated spam to account for 60% of all e-mail traffic.

25. The second set of figures were based on the numbers of spam being reported to enforcement bodies operating "spam-boxes"[1] in the United States and France. These figures were much lower, estimating spam to account for two out of every 100 000 (.002%) e-mails in the United States and 50 out of every 100 000 (.05%) in France. The speaker explained that he calculated these percentages by simply dividing the total number of spam reported to the enforcement bodies by the estimated levels of e-mail traffic. He suggested that one reason these figures were so much lower than the first set was that recipients of spam were not reporting the spam they received, perhaps because they were not aware of where to report it. It was also noted that the first set of figures represented e-mails that had been blocked by filtering software at the Internet service provider (ISP) level before reaching the intended recipient, whereas the second set were based on e-mails that had made it through these filters and been received by users.

26. Commenting on different approaches to measuring spam, one panellist later stated that in the course of conducting measurement studies he found the survey-based approach to be flawed because it involves a subjective judgement on behalf of the participants surveyed. He found technical means for measuring spam (such as filters) to be more objective and, thus, more accurate. He suggested that common standards for measuring spam among governments could facilitate co-operation in fighting spam.

27. In terms of the form of spam, one speaker noted that spam has moved from 100% ASCII (American Standard Code for Information Interchange) to 75% HTML (HyperText Markup Language). Very often, he continued, the body of a spam e-mail will contain no more than a URL (universal resource locator). It is also common for the content of spam or the HTML code to be randomised in order to defeat filters. Re-iterating the point made in Part 1 of the session, he remarked that approximately 90% of all spam messages contain some sort of forgery in the headers. He explained that this was because the current e-mail protocol was designed in the 1980s when forgery or identity (ID) theft was not contemplated.

Session 2: Economic and societal impacts of spam

28. This session focused on the economic and societal costs of spam to all categories of Internet users, as well as network administrators and service providers.

1. "Spam boxes" collect spam forwarded by individual recipients and are used to pursue law enforcement actions against the senders of the spam.

29. The speakers agreed that there is a dearth of good data on the precise costs of spam and that many of the existing studies had problems of methodology. Nonetheless, they said it was clear that spam was imposing serious costs on all categories of Internet users. The speakers noted that, much like environmental pollution, spam imposes a negative externality with its economic damage and costs borne by third parties.

30. Some of the particular impacts highlighted by the speakers and panellists included:

- Increased costs to Internet and e-mail service providers resulting from consumption of network bandwidth, storage space, and computing resources; and loss of reputation and goodwill if they cannot stop spam or properly handle complaints.
- Increased costs to businesses associated with lost worker productivity, degraded network performance, security risks, and waste of system administrator and technical support time.
- Higher communications and data storage charges for individuals, distress or economic loss caused by spam messages which are illegal, fraudulent, deceptive or inappropriate for young children, as well as a loss of privacy particularly relating to the collection and sale of e-mail addresses.
- A negative impact on the security of information systems and networks caused by spam which is used to spread viruses and worms or to perpetrate denial of service attacks.

31. Overall, there was concern that these problems are undermining trust and confidence in the online environment and negatively affecting the reliability and convenience of e-mail. One speaker noted that, in addition, these problems may damage the potential of the Internet to deliver government services (e-government) or the value of the Internet as a forum for political speech.

32. There was a consensus among speakers and panellists that more accurate and regular numbers were needed on the costs and impacts of spam in order to supplement the "snapshot" views that are available now. It was suggested that there were a number of advantages to having these numbers: they can be used to put pressure on governments and the private sector to deal with the problem; they can identify risks for potential targets thus providing an incentive to act; they can identify who is bearing the biggest cost; and they can help determine what the solutions may be.

33. On the issue of possible solutions, one speaker made the point that the solutions to spam should not impose any further costs on the recipients of spam. In particular, he noted with concern that many of the proposed solutions focused on new means of authentication or verification online and worried that this may have deleterious effects on individuals' privacy rights and on the open character of the Internet. He suggested that if authentication was going to be put in place it should only be required for bulk senders of e-mail and not individual users.

Session 3: Technical and business aspects of spam

34. This session examined the mechanics and business models of spam. Speakers and panellists focused on how the spam business is conducted profitably and on some of the technologies being used by spammers.

35. In terms of the spam business model, it was noted that spammers make money based simply on bulk. As there is little or no cost associated with sending e-mail, spammers can make a profit even with a very low response rate. It was noted that spammers also make money by perpetrating fraud. One speaker referred to the increase in "phishing" attacks which can result in particularly high yields. Phishing is a practice whereby spammers send out "spoofed" e-mail messages pretending to be a business or an

institution with whom the recipient already has a relationship (*e.g.* a retailer, e-mail service provider, financial institution). These e-mails contain falsified return addresses, links, and company branding and are intended to fool the recipients into disclosing personal or financial information such as account usernames or passwords, credit card or bank account numbers. The speaker added that "phishing" scams are becoming more and more sophisticated and as a result have a response rate of up to 20%.

36. There was a presentation on the mechanics of spam using Japan as an example. The majority of spam in Japan is sent to mobile phones and involves either advertising for "dubious dating sites" or demands for payments of false invoices. There are three categories of players involved in sending this spam – the site operators (who initiate the sending of spam in order to attract visitors to their sites), the address list developers (who have a number of techniques to harvest valid e-mail addresses, either by conducting mass mailings online or culling from public sources), and finally the transmitters (who take orders from site operators and send out spam either via the Internet or mobile networks). Initially spam was sent to mobile phones via the Internet. The adoption of filter functions (filters that only permit incoming mail from user-designated domains) greatly reduced spam for some time. However, spammers eventually developed new means of sending out spam through mobile phone networks including to users of the filter function. The mobile providers responded to this new practice by deactivating accounts being used to send spam and setting limits on the numbers of e-mail that could be sent from phones. Again this had a temporary effect of reducing spam, but spammers continued to search for new methods and have recently started spamming through short message services (SMS). The presenter described the continual battle between spammers to find new technological means to send spam and the regulators or network operators to find new tools to block spam as a "cat-and-mouse game". He also remarked that much of the spam in Japan was now coming from overseas and stressed the need for co-operation and sharing of best practices in the telecommunications industry.

37. One audience member referenced a report from Spamhaus (an anti-spam organisation) which estimates that 90% of the spam received in North America and Europe is sent from a core group of 180 serious spammers. He questioned why if there were so few spammers operating that they could not be found. In response, one panellist noted that spammers have a number of means (*e.g.* false headers, open relays) to obscure their identities, making it very difficult to locate and hold them accountable for their practices. The panellist suggested that one possible way to locate these spammers was to set up sting operations on open relays to record incoming IP (Internet protocol) addresses.

38. In preparation for the following session, there was also an introductory discussion of measures that can be taken to make the costs of spamming more prohibitive while increasing trust in legitimate e-mail. One panellist referenced two different kinds of self-regulatory schemes for senders of commercial e-mail. Under the first, "trusted sender" scheme, commercial e-mailers sign up to a third party service which certifies the legitimacy of their e-mail campaign and tags their e-mails for recognition by ISPs. Under the second "bonded sender" scheme, commercial e-mailers post a financial bond with a third-party service as a guarantee for assured delivery by ISPs. This bond is debited if the participating sender fails to abide by the third party's standards or if there are excessive consumer complaints against the sender. The thinking is that as more and more legitimate companies sign up to these kinds of schemes, spammers will become increasingly marginalised and more easily filtered by ISPs.

Session 4: Technical solutions

39. Closely related to the previous discussion, this session explored what technical solutions are available to businesses, ISPs, and individuals to combat spam. Speakers described existing technical solutions, such as filtering and blocking programs and examined the effectiveness of these solutions. There was also a discussion of possible future solutions, such as structural changes to e-mail.

40. One speaker gave a presentation on a commercial anti-spam service for businesses. This service works by screening all incoming mail against public blacklists (lists of IP addresses of known spammers) and against private, customer configured blacklists or whitelists (lists of trusted IP addresses). In addition, e-mail from unknown sources are scanned using hundreds of rules (heuristics) which analyse the probability of the e-mail being spam. The speaker noted that this service is currently only available for business users but that there were plans to make it available to ISPs at some stage in the future.

41. There was general agreement that ISPs need to be the first line of defence in combating spam. One speaker noted that the Internet Engineering Task Force's (IETF) Network Working Group has developed protocol standards (RFC 2821) and best practices (RFCs 2505 and 2635) for ISPs to follow in order to help reduce levels of spam. Among other things, these documents require ISPs to prevent their mail servers being used to relay e-mails from unauthorised third parties and to provide sufficient information in e-mail headers to make it possible to trace the source of e-mail. They also advise that ISPs should have the capability to accept or refuse mail from a specific host or group of hosts, and to use reverse DNS lookups to verify the legitimacy of the sending domain.

42. It was noted that in addition to these technical standards, ISPs routinely filter and block spam at the network level. For example, AOL typically blocks between 1.5 billion and 2 billion spam e-mails per day at the network level. This amounts to between 70% and 80% of total e-mail received by AOL. However, it was also stressed that this kind of filtering and blocking will always result in false positives. It was suggested that, for many users, missing legitimate e-mail is a potentially more serious problem than receiving spam. One speaker thus remarked that a more viable solution to spam in the long-term was to develop a new protocol for e-mail that could authenticate senders.

43. Speakers and panellists also emphasised the role of the individual user in combating spam. It was suggested that users need to be better educated about basic technical measures to protect themselves against the harmful effects of spam, such as installing firewalls and anti-virus software.

44. The question was asked whether there was any focus on preventing spam at the level of the originating rather than receiving server. It was noted that most ISPs include provisions in their "acceptable use" policies or "terms of service" agreements that prohibit the use of their resources for sending bulk unsolicited mail. Breach of these provisions will usually result in suspension or termination of service. It was suggested that industry self-regulation would be helpful in this area to streamline terms of service agreements and to encourage ISPs to conduct surveys of their own networks and take appropriate action against spammers operating within those networks.

Session 5: Regulation and self-regulation

45. This session focused on existing regulatory and self-regulatory efforts to combat spam with particular attention to the international dimension of these measures. Speakers and panellists considered the elements of effective regulation and self-regulation, and discussed the overall advantages and limitations of these measures.

46. A number of speakers stressed the need for regulation to ensure that countries do not become safe havens where spammers can operate with impunity. It was also noted that regulation is useful to provide both a framework for other anti-spam efforts and a legal basis for international co-operation. The point was made that in crafting anti-spam laws there are a number of competing factors and considerations. For example, one must be careful not to stifle legitimate business activities or free speech online. A number of speakers mentioned the need for the law to be sufficiently flexible and technology neutral in order to allow for the continued development of new anti-spam measures by the private sector and government. It was also recommended that regulation grant ISPs a right of action against spammers, as private actions can play

an important role in supplementing official enforcement actions and imposing financial penalties on spammers. Finally, the importance of designating one lead agency to be responsible for enforcing the law was emphasised.

47. Speakers recognised that, given the cross-border nature of the spam problem, some form of international co-operation was nearly always necessary in order to enforce national laws. However, also it was noted that this does not mean that there has to be absolute uniformity among national laws. As an example, one speaker referenced the Memorandum of Understanding (MOU) on spam between Australia, where the law requires opt-in consent for unsolicited e-mails, and Korea, where opt-out consent is required.

48. There was a consensus that while regulation is a key component of an effective anti-spam strategy, it is not a panacea. It was noted that self-regulation by industry would always be necessary to deal with spam originating in countries where there is no legislation or where the legislation is substantially different. One speaker gave examples of self-regulatory initiatives by European telecommunication providers, including the development of black lists, implementation of codes of conduct, use of filters for incoming and outgoing mail, and widespread awareness campaigns to educate and empower users. Reference was also made to a forthcoming agreement between the national data protection officers in Europe and the direct marketing associations to lay down specific rules for e-mail marketers. This agreement is to be modelled along the Code of Practice on the use of personal data in direct marketing which was adopted in June 2003 by the European data protection commissioners. One panellist, however, expressed scepticism about self-regulatory efforts saying that based on his experience in the United States they were rarely successful without strong enforcement mechanisms backed by government oversight.

49. A question posed was why spam continued to proliferate in spite of all the numerous regulatory and self-regulatory measures being put in place. In response, speakers and panellists referenced the difficulty of enforcing national laws across borders, noting that most spam is sent from offshore accounts. They also focused on the need to reduce the economic incentive of spamming, for example, by including stricter penalties in anti-spam laws or by imposing a cost on bulk senders of e-mails.

Session 6: International law enforcement co-operation

50. Building on the previous discussion, this session highlighted the need for effective law enforcement co-operation in investigating and prosecuting spammers. Focusing on the difficulties that law enforcement faces in locating spammers, establishing jurisdiction and enforcing remedies, speakers and panellists agreed that international co-operation is essential to the success of any anti-spam strategy.

51. One speaker noted that in conducting investigations it is important to look both backwards and forwards in order to find the identity and location of the spammer. Looking backwards, investigators try and determine where the e-mail originated by relying on headers and routing information in the e-mail itself. Looking forwards, investigators often concentrate on the “call to action,” that is, the place where recipients are being directed or what they are being asked to do. As most spam requires some sort of financial transaction, he said, the guiding principle in these investigations is to “follow the money.” Investigations usually reveal an international dimension to spam. For example, spam often originates from, or is routed through, overseas servers, or the proceeds of spam are transferred to an offshore account. For this reason, he said, law enforcement needs to have adequate powers at the national level to either conduct or assist in cross-border investigations and prosecutions.

52. There was agreement that the *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* could provide a useful framework for effective international co-operation on spam. In addition, a number of speakers noted that there are existing

networks at the international or regional level which can be employed to facilitate co-operation in this area. They referenced, for example, the International Consumer Protection and Enforcement Network (ICPEN) which facilitates the exchange of information among consumer enforcement bodies; the European Conference of Data Protection Commissioners which has developed a system for cross-border complaints handling; and the Nordic Consumer Ombudsmen who have signed an agreement on co-operation in initiating lawsuits and information sharing. One speaker also referenced two important proposals, at the US and EU level, which would provide new tools for law enforcement co-operation in cases involving cross-border fraud, including fraudulent spam. In the United States, the proposed International Consumer Protection Act would empower the US Federal Trade Commission (FTC) to provide investigative assistance to foreign agencies; to gather more information from third parties and foreign agencies; and to negotiate international agreements. The law would also clarify the FTC's jurisdiction to take action and obtain remedies in cross-border cases. At the EU level, the proposed Regulation on Enforcement Co-operation would empower national consumer protection authorities to share information and to request enforcement action from their counterparts in other member states. While these new regimes for co-operation could not cover all cases of spam, they would at least apply to some of the most egregious forms involving fraud or misleading or deceptive advertising.

53. The point was made that co-operation on spam is complicated by the fact that the types of bodies responsible for enforcing anti-spam laws vary widely from country to country. For example, responsibility may lie with data protection authorities, consumer protection agencies, telecommunication regulators, criminal authorities or a combination of these. Speakers noted, therefore, that a necessary first step to co-operation is to develop a contact list clearly identifying the competent authority or authorities in any given country.

54. The need for improved co-operation and information sharing between governments and the private sector was also emphasised. A number of speakers noted that industry is well placed to assist law enforcement efforts by providing information on spammers' techniques and practices. For example, one speaker referenced the recent co-operative effort between the New York Attorney General's Office and Microsoft to investigate and take legal action against one of the world's biggest spammers. Speakers suggested that ISPs, businesses, and financial institutions needed to be encouraged to report spam. The comment was made that one of the main difficulties in this regard at the moment was that businesses did not know who to contact within their national governments. It was recommended that governments should create a single point of contact so that businesses could report spam and provide information on where attacks are taking place.

Session 7: Awareness and education

55. This session examined how increased consumer and industry awareness, education and best-practice use of electronic communications can minimise the impact of spam. The session highlighted both public and private initiatives to promote awareness among users. Speakers and panellists also discussed what role governments, industry leaders and civil society should play in creating and widely disseminating anti-spam resources and educational guides.

56. There was a presentation on a business initiative to create an online resource on spam aimed at educating users about how to appropriately and responsibly deal with spam or how to avoid receiving it in the first place. The resource site is bilingual (English and French) and currently contains an inventory of contact points in countries around the world where users can report or opt-out of unsolicited messages. The resource will soon also contain practical advice for users to avoid receiving unwanted commercial e-mail (for example, not posting e-mail addresses on the web, using more complicated e-mail addresses, installing spam filters and other software solutions). The speaker emphasised the need for governments to play a role in promoting awareness. He recommended increasing the transparency of anti-spam resources (such as

those on government Web sites); making these resources available in more than one language; and working with the private sector to increase dissemination of resources.

57. Two other specific awareness initiatives were referenced by panellists as good models for future anti-spam campaigns. The first is a campaign, part-funded by the European Commission, to promote safer use of the Internet for the benefit of children and young people. The campaign is run by public and private partners at the national and European level. It disseminates targeted information to various groups such as educators, parents, social workers, librarians, consumer associations, and children. It also seeks to work collaboratively with industry, government and the media to facilitate the exchange of information and awareness material. The second campaign is one being run by a national government, in co-operation with private industry, with the goal of increasing awareness of computer and network security issues, including the risks of malicious spam spreading worms and viruses. As part of this campaign, the government designated one day as a national "information security" day during which it planned: to distribute copies of an information security guide directly to more than 1 million homes; to run advertisements for network security on the front pages of all major daily newspapers and on MTV; and to host briefings on information security in large shopping centres.

58. There was a discussion of what businesses can do to educate their workers about the risks of spam. One panellist made the point that businesses are increasingly concerned with lost worker productivity and are thus more prepared to dedicate time and resources to education and awareness campaigns. One suggestion was for businesses to hold lunchtime seminars or include informational material on spam with employees payslips.

59. There was agreement that individual users have a role to play in combating spam but that the burden of promoting awareness and education should rest with governments, industry, and consumer groups or user organisations. One audience participant raised concern that users were being given mixed messages and suggested that there should be more co-ordination in educational initiatives. For example, he noted that during the previous sessions there was a difference of opinion even on simple questions such as whether to respond to spam with a request to unsubscribe. Some speakers cautioned against responding to spam saying that it only validates the recipient's e-mail address and thus results in more spam. Others stated that while such efforts may be futile (in that they are ignored or the return e-mail address provided is not valid) they do not result in increased levels of spam. Another speaker attempted to clarify this matter noting that there had been a change of practice in spamming techniques and that most spam now contain web-beacons and other "spyware" that make it possible to verify an e-mail address once the recipient simply opens the spam e-mail. As a result, spammers no longer need to reply on unsubscribe requests to validate e-mail addresses. He remarked that users now need to be educated to recognise and delete spam e-mails without even opening them.

Session 8: Evaluating current approaches and looking ahead

60. This session examined what governments, businesses and consumers have been doing individually and collectively to address spam. Panellists evaluated current approaches and discussed possible areas for further work.

61. Speaking on technological approaches, one panellist suggested that filtering programs had made a lot of progress but that improvements were still needed, for example, by making them more multilingual to respond to the increase in Asian and other non-roman characters sets. He said that it also seemed essential to introduce the concept of authentication or validation into e-mail. He stressed that when industry speaks of authentication or validation systems it is only contemplating their use for large senders of e-mail. However, he also suggested that it may be useful to raise awareness that every server has the capacity to provide authentication or validation and that those who want more security can take advantage

of this option. Speaking more generally, he remarked that many of the solutions to spam were being applied retroactively and in isolation. He recommended a more proactive approach that would look at the incentives and other causes of spam rather than just its symptoms. He recommended more co-operation between the public and private sectors. For example, he said, there needs to be better information sharing in the area of enforcement. Industry can facilitate enforcement actions if it knows what kind of information is most useful in bringing a case against a spammer and where in government to report this information.

62. Focusing on the consumer perspective, another panellist cautioned against placing too much responsibility on user awareness and "self-help" remedies, stressing the need to harmonise anti-spam laws to provide the highest protection for e-mail users against unwanted intrusions into their private lives. The panellist expressed a strong preference for the EU's opt-in approach to unsolicited commercial e-mail and hoped that it would go a long way towards reducing levels of unwanted messages. In addition, it was argued that one effective way to create a financial disincentive to spammers would be to grant individuals a private right of action. The view was expressed that self-regulatory approaches would do nothing to stop the huge levels of spam coming from "bad actors" who are not sensitive to negative publicity or loss of goodwill.

63. The point was made that there needed to be more co-operation within, as well as between, national governments. One panellist noted that in the United Kingdom for example, it is the Information Commissioner's Office that has responsibility to enforce the law against unsolicited commercial e-mails but that it does not have jurisdiction over fraudulent or deceptive e-mail, which is a matter for the Office of Fair Trading. This panellist also stressed the need to ensure that any solutions to spam are respectful of those individuals who are law-abiding and sending only small numbers of e-mails.

64. There was a discussion about the distinction that seemed to be made throughout the workshop between "legitimate" and "illegitimate" spam, that is, spam which is merely unwanted versus spam that contains fraudulent, harmful or illegal content. Panellists debated whether it was correct at this stage to focus primarily on combating the illegitimate spam. One panellist recommended this approach but stated that this did not mean that there would be no steps against non-permission based marketing. Another suggested that all unwanted e-mail be restricted equally saying that users do not like spam whether it is coming from "crooks" or "big business".

Session 9: Next steps

65. This session focused on the global dimension of spam with a view to determining next steps at the international level. Building on the discussions in their respective sessions, session chairs considered potential long and short tem solutions to the problem of spam as well as the role international organisations, such as the OECD, can play in facilitating globally co-ordinated action.

66. As regards long-term solutions, a number of speakers mentioned the need to study and implement authentication schemes to prevent spammers from forging e-mail headers. Until this underlying problem is addressed, they said, spammers will continue to invent or steal e-mail addresses making them difficult to trace and enabling damaging phishing attacks. In addition, there was a clear interest in further study of the spam business model in order to get a better idea of economic incentives and operational methods of spammers. Speakers suggested that by identifying the various actors involved in the spam business (*e.g.* those who commission, conduct or facilitate spamming), it would be easier to pre-emptively apply economic disincentives and to focus enforcement efforts. The idea of introducing payment mechanisms for large senders of e-mails was again proposed.

67. In the short term, there was agreement that there needs to be vigorous enforcement of anti-spam laws. In this regard, speakers reiterated the need for international co-operation among law enforcement

agencies and for more effective public-private partnerships. They noted that frameworks for international co-operation already existed (*e.g.* in the areas of cross-border fraud and cybercrime) and suggested that these could be applied, or used as models, for co-operation against spam.

68. There was a consensus that the OECD has the experience and expertise to effectively co-ordinate work on spam. In addition to the suggestions mentioned above, participants proposed that the OECD: develop networks with non-member economies to stop them becoming safe havens for spam; assist international law enforcement co-operation by creating contact lists for competent authorities within member countries; foster public-private partnerships to facilitate information sharing; develop best practice guides for online marketers and for ISPs; develop and widely disseminate educational and awareness materials; and review the effectiveness of different approaches to combating spam.

69. **Mr. Takayuki Matsuo**, Director, Directorate for Science, Technology and Industry, OECD closed the workshop by thanking speakers, panellists, moderators, and participants for their active contributions during the workshop and also the European Commission for hosting the event.

70. He singled out the chairs of the three OECD committees working on spam for special thanks. He remarked that their continued leadership would be needed to carry out work in this important area. He noted that the OECD was already planning to organise a second workshop to be hosted by Korea in the autumn of 2004. In the interim, he said, the three committees would be asking member countries to agree on a concrete plan for future steps that involves all stakeholders and that builds on their expertise and existing work in the areas of consumer protection, security and privacy, and communications infrastructure.

71. Mr. Matsuo remarked that the aim of the OECD was to supplement ongoing efforts against spam at the domestic and regional levels with a truly international and interdisciplinary approach. He concluded that by bringing together representatives from governments, business and civil society from around the world, this workshop was an excellent first step in that direction.

OECD

WORKSHOP ON SPAM

2-3 February 2004
Room 0A, Centre Albert Borschette
European Commission, Brussels, Belgium

ANNOTATED PROGRAMME

OECD WORKSHOP ON SPAM

2-3 February 2004

Room 0A, Centre Albert Borschette, European Commission, Brussels, Belgium

This workshop has been organised by the OECD and is hosted by the European Commission, Information Society Directorate-General. The **objective** of the workshop is to explore the growing problem of spam, with a focus on the international dimension. Participants will:

- Discuss statistics, sources and characteristics of spam.
- Examine the variety of approaches to combat spam.
- Examine the degree to which these approaches have been successful.
- Consider next steps with a view to increasing international co-operation to address the issue.

The first day will feature presentations and discussions which will focus on understanding spam and its impact. Day two will turn the discussion towards approaches for combating spam and will conclude with a discussion of next steps.

The **format** of the workshop will mix presentations and moderated panel discussions with an opportunity for questions from the participants in the audience. Panel discussions will be moderated by the session chair and typically involve each of the presenters for the session along with 2-3 additional panellists chosen to ensure balanced viewpoints and expertise. Panellists will be expected to engage the questions posed by the session chairs, or by the audience.

Presenters and panellists have been invited from government, industry, civil society and academia. **Participation** in the workshop is open to the public, but requires advance registration and is limited by available space. Interested journalists will be able to attend.

Please note that PowerPoint presentations will not be made available during the workshop, but will be posted on the OECD Web site at www.oecd.org/sti/spam following the event.

OECD WORKSHOP ON SPAM

2-3 February 2004

Room 0A, Centre Albert Borschette, European Commission, Brussels, Belgium

DAY 1	Monday, 2 February 2004
08.00-09.00	Registration
09.00-09.30	WELCOME AND INTRODUCTION
09.30-11.00	SESSION 1: UNDERSTANDING SPAM
11.00-11.30	Refreshment
11.30-12.30	SESSION 1: UNDERSTANDING SPAM (continued)
12.30-14.00	Lunch hosted by the European Commission
14.00-15.30	SESSION 2: ECONOMIC AND SOCIETAL IMPACTS OF SPAM
15.30-16.30	SESSION 3: TECHNICAL AND BUSINESS ASPECTS OF SPAM
16.30-16.45	Refreshment
16.45-18.00	SESSION 4: TECHNICAL SOLUTIONS
18.00-19.30	Cocktail hosted by the European Telecommunications Network Operators' Association, ETNO
DAY 2	**Tuesday, 3 February 2004**
08.00-08.30	Registration
08.30-10.45	SESSION 5: REGULATION AND SELF-REGULATION
10.45-11.00	Refreshment
11.00- 13.00	SESSION 6: INTERNATIONAL LAW ENFORCEMENT CO-OPERATION
13.00-14.30	Lunch break
14.30-15.15	SESSION 7: AWARENESS AND EDUCATION
15.15-16.00	SESSION 8: EVALUATING CURRENT APPROACHES AND LOOKING AHEAD
16.00-16.15	Refreshment
16.15-17.15	SESSION 9: WHAT ARE THE NEXT STEPS?
17.15	CLOSING

OECD WORKSHOP ON SPAM

DAY 1	**Monday, 2 February 2004**

09.00-9.30 WELCOME AND INTRODUCTION

Commissioner Erkki Liikanen, Enterprise and Information Society, European Commission

Mr. Herwig Schlögl, Deputy Secretary-General, OECD

9.30-11.00 SESSION 1: UNDERSTANDING SPAM

Session 1 Chair: Mr. Andrew Konstantaras, Internet Law and Policy Forum

Although spam has become an everyday feature of online life, there is no widely accepted definition of spam. Spam varies greatly in content, form and originating source. It ranges from advertisements for goods and services, to the promotion and distribution of adult content and illegal material, to solicitations for fraudulent schemes. As spam is carried over global networks it can originate from any country in the world where there is Internet access.

In Part 1 of this session, government, consumer and industry representatives will identify the common characteristics of spam in an attempt to improve our understanding of the problem. Specific questions to be addressed include:

(1) What is spam and how does it differ from legitimate e-mail marketing?

(2) What are the most common types of spam messages?

(3) Who is sending spam and from where?

(4) How do consumers perceive spam?

Speaker 1: Mr. J. Howard Beales, III, Federal Trade Commission, United States

Speaker 2: ***Mr. Patrick von Braunmühl, Federation of German Consumer Organisations***

Speaker 3: ***Mr. Charles A. Prescott, The Direct Marketing Association, Inc.***

Panel discussion between the speakers above and the panellists below, moderated by the Session 1 Chair

Panellist 1*: Mr. Kazuyoshi Maekawa, Fujitsu Ltd.*

Panellist 2*: Mr. Eric Walter, Office du Premier ministre, Direction du développement des medias, France*

11.00-11.30 Refreshment

11.30-12.30 SESSION 1: UNDERSTANDING SPAM (continued)

Part 2 of this session will focus on current efforts to measure spam and its rate of growth. Such efforts are important in order to determine the effectiveness of anti-spam measures. This part of the session will outline existing approaches to measuring spam and evaluate their accuracy and reliability. It will also discuss whether more work in this area would be useful, keeping in mind the challenges posed by varying definitions of spam.

Speaker 4: ***Mr. Enrique Salem, Brightmail***

Speaker 5: ***Mr. Jean-Marie Nivlet, Office du Premier ministre, Direction du développement des medias, France***

Panel discussion between the speakers above and the panellists below, moderated by the Session 1 Chair

Panellist 3*: Mr. Isao Kasubuchi, Ministry of Economy, Trade and Industry, Japan*

Panellist 4*: Mr. Duck-Kyu Joo, Korea Information Security Agency, Korea*

12.30-14.00 Lunch hosted by the European Commission

OECD WORKSHOP ON SPAM

DAY 1 Monday, 2 February 2004

14.00-15.30 SESSION 2: ECONOMIC AND SOCIETAL IMPACTS OF SPAM

Session 2 Chair: Commissioner Mozelle W. Thompson, Federal Trade Commission, United States, Chair of the OECD Committee on Consumer Policy

Spam impacts all categories of Internet users, from individuals, to businesses and governments, as well as network administrators and service providers. It imposes significant costs, both economic and societal, on each of these categories. Every day users and network administrators waste valuable time managing and deleting unwanted messages. This results in lost productivity, higher access charges, and a drain on technical support services. Spam consumes resources, such as network bandwidth, storage space, and computing power, without compensation or consent. Spam also poses serious threats to network security and the reliability of Internet communications. It results in system crashes and is being increasingly used as a vehicle for the spread of computer viruses and worms. Furthermore, the content of spam is often illegal, fraudulent or deceptive, resulting in economic losses and distress to consumers. Finally, the practice of spamming and, in particular, the manner in which e-mail addresses are collected or sold raises a number of privacy concerns. Overall, these problems lead to a loss of consumer trust and confidence in the Internet online marketplace and negatively affect the growth of the digital economy.

This session will explore these and other costs associated with spam, keeping in mind the principles of consumer protection, privacy protection and network security, as set out in various OECD guidelines. Particular issues to be highlighted include:

(1) The impact of spam on individual recipients.

(2) The impact of spam in the workplace.

(3) The impact of spam on critical infrastructures and network security.

(4) The impact of spam on legitimate online marketers.

(5) The broader impact of spam on trust and confidence in the Internet and the growth of the digital economy.

Speaker 1: ***Mr. Marc Rotenberg, Electronic Privacy Information Center***

Speaker 2: ***Mr. Dimitri Ypsilanti, OECD***

Panel discussion between the speakers above and the panellists below, moderated by the Session 2 Chair

Panellist 1: ***Ms. Dorothea Zechmann, T-Online International AG***

Panellist 2: ***Mr. Gianluca Esposito, Council of Europe***

Panellist 3: ***Ms. Katarina de Brisis, Ministry of Trade and Industry, Norway***

Panellist 4: Mr. Jeremy Beale, Confederation of British Industry

OECD WORKSHOP ON SPAM

DAY 1	**Monday, 2 February 2004**

15.30-16.30 SESSION 3: TECHNICAL AND BUSINESS ASPECTS OF SPAM

Session 3 Chair: Mr. Brian Stewart, Permanent Delegation of Australia to the OECD

The very low marginal cost of sending bulk e-mail means that spammers can make a profit despite extremely low response rates. Relying on tools such as automatic harvesting programs and dictionary attacks, spammers have developed numerous ways to collect and/or guess e-mail addresses. In addition, by relying on technical measures such as false headers, mail relays, and spoofing, spammers can obscure their identities making them difficult to locate and to be held accountable.

This session will examine the mechanics of these new technologies and the business models of spam. Setting the scene for the following session, there will also be an introductory discussion of technical measures that can be taken to counteract spam. Key questions to be addressed include:

(1) How do spammers obtain e-mail addresses?

(2) How do spammers remain undetected?

(3) How is a spam business conducted profitably?

(4) How are changing technologies leading to new opportunities for spam (*e.g.* spam via SMS or instant messaging)?

(5) How can new technologies and policies lead to opportunities to stop spam and increase trust in e-mail?

Speaker 1: ***Mr. David Jevans, Anti-Phishing Working Group***

Speaker 2: ***Mr. Kenichi Mori, NTT DoCoMo, Inc.***

Panel discussion between the speakers above and the panellists below, moderated by the Session 3 Chair

Panellist 1: ***Mr. Mike Galvin, BT***

Panellist 2: ***Ms. Fran Maier, TRUSTe***

16.30-16.45 Refreshment

OECD WORKSHOP ON SPAM

DAY 1	**Monday, 2 February 2004**
16.45-18.00	**SESSION 4: TECHNICAL SOLUTIONS** ***Session 4 Chair: Mr. Wonki Min, Ministry of Information and Communication, Korea, Chair of the OECD Working Party on Telecommunications and Information Services Policies*** Closely related to the previous discussion, this session will explore what individuals, businesses and ISPs can do at the technical level to combat spam. Speakers will describe existing different technical solutions, such as filtering and blocking programs. They will examine the effectiveness of these solutions and discuss the possibility of future solutions, such as structural changes to e-mail. In particular, the following questions will be addressed: (1) What kinds of tools are currently available at the end user and ISP level? (2) How effective have these tools been to date and how could their effectiveness be improved? (3) What are the disadvantages and problems associated with these tools (*e.g.* costs, false positives)? (4) How can further development and use of these tools be encouraged? ***Speaker 1***: ***Mr. Christian Rogan, MessageLabs Ltd.*** ***Speaker 2****:* ***Mr. Stephane Marcovitch, EuroISPA*** ***Speaker 3***: ***Ms. Lori Friedman, AOL (UK) Ltd.*** **Panel discussion** with above speakers, moderated by the Session 4 Chair
18.00-19.30	**Cocktail hosted by the European Telecommunications Network Operators' Association**

OECD WORKSHOP ON SPAM

DAY 2 Tuesday, 3 February 2004

08.30-10.45 SESSION 5: REGULATION AND SELF-REGULATION

Session 5 Chair: Mr. Michael Geist, University of Ottawa

More and more OECD member countries have laws in place that directly or indirectly regulate spam. Specific anti-spam laws generally either impose labelling requirements; prohibit the transmission of bulk or commercial messages without the consent (opt-in or opt-out) of the recipient; or ban the use of "spamware". In addition to regulatory approaches, a variety of self-regulatory measures are being put in place by industry groups. For example, a number of online marketing associations operate opt-out lists for users and have developed voluntary codes of conduct for their members based on permission-based marketing. Similarly, mobile telecommunication associations are implementing self-regulatory codes setting acceptable standards for marketing to wireless mobile devices.

This session will describe and discuss existing regulatory and self-regulatory efforts to combat spam, with particular attention to the international dimension of these measures. Specific questions to be addressed include:

(1) What are the main elements of anti-spam laws and how successful have they been?

(2) What other kinds of laws are being applied to spam (*e.g.* data protection and deceptive or unfair marketing laws)?

(3) What kinds of self-regulatory programs are in place, and how successful have they been?

(4) What are the main limitations of regulatory and self-regulatory measures, given the cross-border nature of the problem?

Speaker 1: ***Mr. Lindsay Barton, National Office for the Information Economy, Australia***

Speaker 2: ***Ms. Patricia M. Sefcik, Department of Commerce, United States***

Speaker 3: ***Mr. Philippe Gérard, European Commission***

Speaker 4: Ms. Cristina Vela, European Telecommunications Network Operators' Association (ETNO)

Panel discussion between the speakers above and the panellists below, moderated by the Session 5 Chair

Panellist 1: ***Mr. Petr Piskula, Ministry of Informatics, Czech Republic***

Panellist 2: ***Mr. Keiichiro Seki, Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan***

Panellist 3: ***Mr. Ken McEldowney, Consumer Action***

Panellist 4: ***Mr. Alastair Tempest, Federation of European Direct Marketing***

10.45-11.00 Refreshment

OECD WORKSHOP ON SPAM

DAY 2	**Tuesday, 3 February 2004**

11.00-13.00 SESSION 6: INTERNATIONAL LAW ENFORCEMENT CO-OPERATION

Session 6 Chair: Mr. André Longuet des Diguères, Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes, France

Spamming is a global problem requiring a global solution. As e-mails can originate or be routed through servers around the world, national efforts to investigate and prosecute spammers are extremely difficult. Problems in locating spammers, establishing jurisdiction and enforcing remedies frustrate attempts to apply national anti-spam laws. In addition, the types of bodies responsible for enforcing anti-spam laws differ from country to country (*e.g.* data protection authorities, consumer protection agencies, telecommunication regulators, and criminal authorities). Effective international law enforcement is therefore difficult, but nonetheless essential to the success of any national regulatory measures.

This session will address international co-operation efforts to enforce laws against spam. Particular issues to be addressed in this session include:

(1) What steps need to be taken at the national level to facilitate more international law enforcement co-operation?

(2) How can the varying types of competent authorities responsible for spam work effectively together?

(3) How can international co-operation and information sharing between governments and the private sector be improved?

(4) What lessons can be drawn from existing measures to enhance co-operation in related areas (*e.g.* cross-border fraud and cyber-crime)?

Speaker 1: Mr. Hugh Stevenson, Federal Trade Commission, United States

Speaker 2: Mr. Giovanni Buttarelli, Data Protection Authority, Italy

Panel discussion between the speakers above and the panellists below, moderated by the Session 6 Chair

Panellist 1*: *Ms. Beatrice Delmas-Linel, Microsoft EMEA

Panellist 2*: *Ms. Victoria Villamar, Bureau Européen des Unions de Consommateurs / European Consumers' Organisation

Panellist 3*: *Mr. Nam-cheol Kim, Ministry of Information and Communication, Korea

Panellist 4: Ms. Marianne Åbyhammar, Swedish Consumer Agency, Sweden

13.00-14.30 Lunch break

OECD WORKSHOP ON SPAM

DAY 2	**Tuesday, 3 February 2004**

14.30-15.15 SESSION 7: AWARENESS AND EDUCATION

Session 7 Chair: Ms. Susan Grant, National Consumers League

This session will examine how increased consumer and industry awareness, education and best-practice use of electronic communications can minimise the impact of spam. The session will highlight initiatives to promote awareness among users and focus on practical steps users can take. In particular, it will consider:

(1) How to reduce the amount of spam received.

(2) How to appropriately and responsibly deal with spam once it is received.

(3) What role governments, industry leaders and civil society should play in creating and widely disseminating anti-spam resources and educational guides.

Speaker 1: Mr. Christopher Kuner, Hunton & Williams, International Chamber of Commerce

Panel discussion between the speaker above and the panellists below, moderated by the Session 7 Chair

Panellist 1: Mr. Hubert van Breemen, Confederation of Netherlands Industry and Employers VNO-NCW, Chair of the Business and Advisory Committee to the OECD Task Force on Consumer Policy

Panellist 2: Ms. Valerie Thompson, European Research into Consumer Affairs

Panellist 3: Mr. Anthony Wing, Australian Communications Authority, Australia

Panellist 4: Ms. Kristiina Pietikäinen, Ministry of Communications, Finland

OECD WORKSHOP ON SPAM

DAY 2	**Tuesday, 3 February 2004**
15.15-16.00	**SESSION 8: EVALUATING CURRENT APPROACHES AND LOOKING AHEAD** ***Session 8 Chair: Mr. Bernd Langeheine, European Commission*** No single solution to the problem of spam, whether of a technical, regulatory or self-regulatory nature, is likely to be successful on its own. A multi-dimensional approach is therefore needed to help eliminate spam. In this session panellists will examine what governments, businesses and consumers have been doing individually and collectively to address spam. Panellists will evaluate current approaches, identify shortcomings in these current approaches, and discuss possible improvements. **Panel discussion** moderated by the Session 8 Chair ***Panellist 1*: *Ms. Jean Ann Fox, Consumer Federation of America*** ***Panellist 2: Mr. Joseph Alhadeff, Oracle Corporation, Chair of the Business and Advisory Committee to the OECD Task Force on Information Security and Privacy*** ***Panellist 3*: *Mr. Phil Jones, Information Commissioner's Office, United Kingdom***
16.00-16.15	**Refreshment**

OECD WORKSHOP ON SPAM

DAY 2	**Tuesday, 3 February 2004**

16.15-17.15 SESSION 9: WHAT ARE THE NEXT STEPS?

Session 9 Chair: Mr. Peter Ferguson, Industry Canada, Canada, Chair of the OECD Working Party on Information Security and Privacy

This session will focus on the global dimension of spam with a view to determining next steps at the international level. Building on the discussions in their respective sessions, session chairs will consider:

(1) The areas where globally coordinated action is most needed (*e.g.* research and information gathering; education and awareness; encouraging self-regulation and the development of interoperable technical solutions; international co-operation in enforcing national laws, or all of these) and how this can best be achieved.

(2) The areas where solutions can be implemented most rapidly.

(3) The role that international organisations, such as the OECD, can play in facilitating such co-operation.

Panel discussion moderated by the Session 9 Chair

Session Chair 1*: *Mr. Andrew Konstantaras

Session Chair 2*: *Commissioner Mozelle W. Thompson

Session Chair 3*: *Mr. Brian Stewart

Session Chair 4*: *Mr. Wonki Min

Session Chair 5*: *Mr. Michael Geist

Session Chair 6*: *Mr. André Longuet des Diguères

Session Chair 7: Ms. Susan Grant

Session Chair 8: Mr. Bernd Langeheine

17.15 CLOSING

Mr. Takayuki Matsuo, OECD