

ITU WSIS THEMATIC MEETING ON COUNTERING SPAM

CONSUMER PERSPECTIVES ON SPAM: CHALLENGES AND CHALLENGES



International Telecommunication Union

This paper has been prepared for the ITU World Summit on the Information Society (WSIS) thematic meeting on Countering Spam, organized under the ITU New Initiatives Programme by the Strategy and Policy Unit (SPU). The paper was written by Marc Rotenberg, Executive Director of the Electronic Privacy Information (EPIC) in Washington, DC, United States, and Samantha Liskow, an EPIC IPIOP Fellow. Further information about spam and privacy may be obtained at the EPIC website at: <http://www.epic.org>.

The meeting project is managed by Robert Shaw (Robert.shaw@itu.int) and Claudia Sarrocco (Claudia.sarrocco@itu.int) of the Strategy and Policy Unit (SPU) and the series is organized under the overall responsibility of Tim Kelly, Head, SPU. This and the other papers in the series are edited by Joanna Goodrick; see www.itu.int/ni.

The views expressed in this paper are those of the author and do not necessarily represent those of ITU or its membership.

1 The scope of the problem

In 2001, the Trans Atlantic Consumer Dialogue (TACD), an alliance of more than 60 consumer organizations in the United States and Europe, recognized that the use of unsolicited commercial electronic communication is a growing burden for consumers who use e-mail. As TACD stated in a joint resolution, “governments need to work together to develop common approaches to address consumer concerns about unsolicited commercial e-mail”. TACD identified a significant distinction between commercial and non-commercial speech and urged the adoption of policies based on prior affirmative consent.¹

In the three years since TACD issued its warning the problem of spam has grown at a dramatic rate. According to a recent survey by Brightmail, 65 per cent of all internet e-mail would now be considered spam. Significantly, the largest categories of spam were for products, which is e-mail advertising general goods and financial services, which include investment opportunities, credit reports, real estate sales, and loans.²

This paper reviews the consumer responses to spam, the efforts of various international organizations, consumer education efforts, as well as proposed policy frameworks.

2 Consumer responses

Consumers are advised to take a number of steps to reduce the amount of spam that they receive. This section reviews those recommendations and explores the practical consequences.

2.1 Reduce posting on publicly accessible websites

Some organizations have recommended that consumers avoid posting e-mail addresses on websites, so that the e-mail address can not be obtained by various e-mail harvesting programs. While it is generally advisable to limit the disclosure of personal information, it is often difficult to do so. Consumers are routinely asked to provide e-mail addresses as part of a website registration process. Businesses also ask for e-mail addresses in the course of online sales and typically use the e-mail address for subsequent marketing. Employers routinely post e-mail addresses for employees. E-mail addresses are also made available through Internet chat and other online services. Even a consumer who takes reasonable measures to prevent the public disclosure of an e-mail address may find it difficult to keep the address off marketers’ mailing lists over time.

2.2 Create multiple e-mail addresses

Many organizations, including the US Federal Trade Commission (FTC) have proposed establishing separate e-mail accounts, apart from personal addresses, to be used for public disclosure or to receive marketing information and other junk mail.³ There are however practical problems with this approach. Consumers may continue to find it difficult to protect their personal e-mail address, for many of the reasons described above. Consumers will also have to track multiple e-mail addresses, in addition to the various privacy rules and expectations that are being used for commercial purposes and to exchange important communications.

2.3 Limit disclosure of e-mail address

Another proposal for consumers to avoid receiving spam is to be aware, when filling out online forms or giving out their e-mail addresses, of how their addresses will be used. Consumers are advised to pay attention to check boxes that request the right to send e-mails to them, or to share their addresses with other parties, and should opt out if they are concerned about dissemination of their addresses. They should also read websites’ privacy policies to determine how exactly their addresses may be used.⁴ Many consumers also find the privacy policies to be inconsistent from one site to the next, particularly in regions of the world where there is no baseline legislation that regulates the collection and use of personal information. Even in those regions where such legislation exists, consumers must also consider whether terms in privacy policies will actually be enforced.

2.4 Use of e-mail filters

Technological methods are also being developed to reduce the amount of spam that a consumer receives. E-mailers now have numerous options available for filtering or blocking spammers who attempt to infiltrate their inboxes. The filters are often provided by ISPs and e-mail services, and programs are also available by

download, some free of charge.⁵ Ideally, the filters would ensure that a consumer receives only desired e-mail, and all other communications would be deposited in the trash. In practice, e-mail filters often produce both *underblocking* and *overblocking*. Underblocking refers to the fact that e-mail filters invariably allow many messages to get through that should otherwise be blocked. Spammers have become particularly adroit at trying to defeat spam filters. They might, for example, avoid the use of text strings that match phrases in a look-up program which would signify spam. “Great Sex” becomes “Great S e ! x.” Spammers will also spoof known addresses, including the address of the e-mail recipient, to deceive an e-mail filter. Of course, spam filters are also becoming more sophisticated and in the battle between spam and counter-spam measures, new techniques are adopted to respond to new forms of spam. Learning heuristics also allow users to develop rule-spam techniques that filter messages from particular users or on particular topics.

The other problem arising from spam concerns overblocking. In this case, an e-mail communication that is labeled as spam is in fact a desirable communication. For example, a spam filter that automatically marks any e-mail with the character “?” in the subject header as spam will designate both the message “Need software? Click here”. And “Should the 4th be happy?” as spam.⁶

In practical terms, sophisticated users of spam will often direct suspected spam to a junkmail folder or “sandbox,” where it can be reviewed prior to deletion. While this process can somewhat reduce the risk of overblocking, it reduces the value of spam filters and will become more time-consuming as the problem of spam accelerates.

2.5 Challenge response techniques

Another approach to spam is to require a user who sends an e-mail to another user to reply to an automatic message before the e-mail is conveyed. The recipient does this to build a list of trusted e-mail senders and to block e-mail from parties who are unknown, or who are unwilling or unable to confirm their identity. Some users have reported success with challenge-response techniques, though there are many obstacles to the widespread adoption of challenge-response, including the use of various techniques and the difficulties of managing large lists.

3 Organizational efforts

But how do consumers learn about anti-spam methods, decide which technologies to use, or feel empowered in any way to understand and cope with spam? Anti-spam organizations around the world are making it a high priority to educate and interact with consumers.

The OECD Directorate for Science, Technology and Industry, in its paper for a January 2004 spam conference, observes that, although legislation may not be able to protect a consumer from a foreign spammer, the education of e-mail users represents a potential cross-border solution.⁷ Similarly, the European Commission, in its discussion of EU Member States’ approaches to spam, stresses the importance of creating “awareness” among users. The Commission recommends that authorities, businesses and consumer associations should ensure that consumers understand the risks of sharing their personal data over the Internet, and provide practical information to consumers about how to avoid spam, what to do when they are confronted with it, and what products and services are available to help.⁸

Many organizations are deeply involved in educating consumers about spam, especially through their websites. The website of the French Data Protection Authority, noted favourably in the reports of both the European Commission and the OECD Directorate, includes published spam reports, information on legal developments, and examples of letters that consumers may model when complaining directly to a spammer.⁹ The US FTC also maintains a website, which offers publications on avoiding unwanted e-mails and “spam scams”, such as the proliferating “phishing” schemes which deceive consumers into providing their financial information.¹⁰ The Australian Government’s Communication Authority provides online advice about how consumers can avoid becoming “accidental spammers”.¹¹ Non-governmental anti-spam groups also educate consumers via the Internet, and particularly active organizations include the Spanish Internet Users Association (“AUI”)¹³, the SpamCon Foundation,¹⁴ and Spamhaus.¹⁵

Some organizations are providing additional resources to consumers. The Singapore AntiSpam Resource Centre website was launched in May 2004 “to provide a central anti-spam repository for the public and industry”.¹⁶ The site includes reviews of anti-spam software, free software downloads, and information about

Singapore's proposal for anti-spam legislation and how consumers can comment on it. The Korean Spam Response Center, established in 2003 by the Korea Information Security Agency, provides an online spam complaint form.¹⁷ The Response Center also develops technical measures, conducts policy studies, interacts with international organizations, and requests legal actions against violators of the Korean anti-spam law.¹⁸

3.1 Role of consumer education

Consumer education may be particularly important for the success of anti-spam legislation. The European Commission stressed that the level of awareness among users about their rights and how to enforce them will be key in producing effective enforcement, and suggested that governments make sure consumers are aware of where they can complain, what will be investigated, what types of action may be taken, and what information they need for authorities to launch an investigation.¹⁹ A good example of such an effort is the UK Information Commissioner's website, which includes guidance documents explaining its country's new regulations implementing the European Community Directive.²⁰

The European Commission also stresses the need for "clarity and coordination" among national authorities.²¹ Countries seem to be increasingly recognizing the need for cooperation and coalition-building both within nations and across borders, as a survey of the following efforts shows.

3.2 National coalitions

- In May 2004, the Canadian Minister of Industry announced the creation of a Spam Task Force composed of experts, ISPs, consumer advocates, and marketing representatives. The Task Force developed a "six-point action plan", which includes among its goals the enhancement of consumer education and awareness, and the promotion of an international framework to fight spam.²² The Task Force will present its findings to the Minister in spring 2005.
- The Internet Society of China, a trade association, has created a blacklist of spam servers. The Society's Anti-Spam Coordination Team, established in 2002, has held workshops, and has begun to block the blacklisted mail servers after a period of non-compliance.²³
- The Hong Kong Internet Service Providers Association developed a "branding scheme": ISPs will be able to use a special logo if they observe an industry code of practice, which involves taking preventive measures against spam and suspending spammers' services.²⁴ The Association works with the Privacy Commissioner and the Office of the Telecommunications Authority.²⁵
- A New Zealand non-profit internet group, InternetNZ, created the Anti-Spam Task Force, of which the country's Direct Marketing Association is a member. The group has met with the Government, sent a member to the OECD Conference on Spam, worked with the press, and held a conference in Wellington in June 2004. The group encourages all ISPs to refer their customers to its website, which includes a discussion of anti-spam legislative activity.²⁶
- The Singapore Information Technology Federation, a group of technology security companies such as Brightmail and Symantec, held an anti-spam forum in June 2004, bringing together government, industry and trade associations, IT companies and academics to discuss legal, policy and technical anti-spam solutions.²⁷

3.3 Cross-border coalitions

- The FTC announced in January "Operation Secure Your Server", an effort by multiple agencies in 26 countries to identify owners or operators of open relay or proxy servers, and to educate businesses about ways to protect their systems. The participating agencies sent letters to identified businesses, and the FTC manages a website for the Operation, which is referenced and linked to by various consumer groups.²⁸
- Econsumer.gov, made up of the OECD and government agencies from 17 countries, provides a web form on which consumers can make cross-border complaints.²⁹ "The information contained in your complaint will allow the government agencies to spot current fraudulent schemes and help us decide how we might take action", reads the website. Econsumer's site also includes links to governmental

agencies, and information about how consumers may resolve their complaints, and is available in English, French, German, Korean and Spanish.

- The Asia Pacific Coalition Against Unsolicited Commercial E-mail (APCAUCE), which includes member groups from Australia, Hong Kong-China, India, Korea, Malaysia and New Zealand, held a Net Abuse Workshop in Kuala Lumpur in February, and is planning a July workshop in Kathmandu, Nepal, and a 2005 workshop in Kyoto, Japan.³⁰

4 Limitations

4.1 Government frustration

Despite efforts by governments and consumer groups to educate and assist e-mail users, and despite increasing amounts of anti-spam legislation, frustration abounds. Philippe Gerard, director general of the Information Society of the European Commission, criticized the lack of cooperation between anti-spam groups at a spam conference in June 2004. “We see different initiatives going in all different directions and the effectiveness is maybe not there”, he said. “We see [spam] as a major threat to consumer confidence, and we see consumer confidence as a pre-requisite for the strong growth of e-commerce”.³¹ British Information Commissioner Richard Thomas also expressed frustration at an April 2004 privacy symposium, and noted both the difficulties of enforcing European anti-spam directive rules, and the absence of an international system to track down violators.³²

4.2 Practical problems

There are also practical problems that consumers face in combating spam. These include the simple economics of the spam problem that shifts costs from the sender to the recipient and makes it inexpensive and relatively easy to send spam to a very large number of Internet users. Unlike traditional junk mail, the marginal cost for each electronic message is essentially zero. Therefore, spammers are as likely to send to a million users as they are to a thousand. But for the recipients and the ISPs, the costs of conveying spam quickly accumulate.

Second, the origin of spam is often difficult to determine. Spammers frequently send messages from domains they do not own and in ways that conceal the source of the message. There are also difficult jurisdictional problems in spam enforcement, including the need to improve coordination among consumer protection and law enforcement agencies, and even the definitional problems concerning what constitutes spam. There are also practical problems that consumers face concerning technical solutions, which are not perfect. As described above, filters both overblock and underblock, and challenge and response may be too cumbersome for many users. Even the reluctance of some groups to support sensible legislative frameworks has contributed to spam problems.³³

Because of these practical concerns, consumer organizations have generally favoured a multi-pronged approach to spam that includes regulatory, technical, and administrative solutions. Consumer organizations in the United States have specifically endorsed a “Policy Framework for Effective Spam Legislation” that recommends: a clear definition of spam, an opt-in standard, a private right of action, technical solutions, international cooperation, opposition to state preemption, and support for “prohibiting false and deceptive headers and subject lines, requiring commercial senders to provide their physical addresses, enabling consumers to opt out easily from continuing to receive commercial e-mails, and setting significant penalties for harvesting e-mail addresses”.³⁴

European privacy experts have also sought to clarify the requirements for compliance with European Directive on Privacy and Electronic Communications. The Data Protection Working Party’s Opinion 5/2004, adopted in February, was meant to clarify of various features of the July 2002 Directive 2002/58/EC that are subject to differences of interpretation.³⁵ Notably, the Working Party attempts to define the requirement that direct marketers obtain “prior consent” from subscribers in order to e-mail them.³⁶ According the Party, consent may be given by a person who registers on a website and is later asked to confirm her consent, or it may be given by general acceptance of the terms of a contract—by the ticking of a box, for instance—as long as the consent is “informed, specific and freely given”.³⁷ Consent is *not* obtained by sending a general e-mail requesting consent, nor by using pre-checked boxes on a website.³⁸ The Party also suggested that “direct marketing” include marketing by charities and political organizations.³⁹

4.3 TACD assessment of anti-spam efforts

Perhaps the most telling and important way to gauge whether anti-spam efforts are succeeding, is to listen to e-mail users themselves. Recent surveys demonstrate widespread dissatisfaction among consumers. At the end of 2003, the Trans Atlantic Consumer Dialogue (TACD) carried out a two-month online survey of over 21,000 people from more than 36 countries. TACD released the results at their 2004 annual meeting—held in Brussels in February.⁴⁰ A majority of respondents (65 per cent) received six or more pieces of spam per day.

The respondents discussed their attitudes towards spam:

Consumer attitudes towards spam

95 per cent either hate spam or were annoyed by it.

83 per cent believe most spam is fraudulent or deceptive.

91 per cent are concerned about children's exposure to spam.

Source : 2004 TACD Survey

The respondents reported the practical effects of spam:

Practical Effects of Spam

66 per cent said that spam cost them or their employer significant time or money.

52 per cent shop less online because of spam.

17 per cent of the people who employed a filter said it worked well.

Source :2004 TACD Survey

And suggested solutions:

Solutions to Spam

84 per cent said that *all* unsolicited commercial e-mails should be banned.

82 per cent said that governments should only allow commercial e-mails to be sent if the consumer has opted in.

80 per cent said it would be helpful if spam was labelled as advertising.

Source: 2004 TACD Survey

The views expressed by consumers in the TACD survey underscore the level of public concern about the spam problem as well as the willingness of consumers to support aggressive action to slow the increase in spam.

4.4 Pew Internet project survey of anti-spam efforts

In the United States, the Pew Internet Project reported in March 2004 that e-mailers' dissatisfaction was higher than the year before, and that the CAN-SPAM legislation had not helped most e-mail users two months after it went into effect.⁴¹ Pew compared e-mailers' attitudes about spam with numbers from its June 2003 survey⁴² and found that dissatisfaction with spam was actually higher in 2004. Sixty-three per cent of e-mail users said that spam made them less trusting of e-mail (up from 25 per cent in 2003) and 29 per cent said that they had reduced their use of e-mail (up from 25 per cent in 2003). Eighty-six per cent of e-mailers reported distress with spam.⁴³

The Pew report also reveals why spam may be so persistent a problem: nine per cent of e-mailers said they had responded to an e-mail that they later discovered was fraudulent, three per cent had provided personal information in response to an unsolicited e-mail, and five per cent of users—representing some six million people—had ordered a product or service connected to an unsolicited e-mail.

4.5 Next steps

An important question then, is what, apart from current efforts, will make a dent in the spam problem. What is the next step? In June 2004, the Federal Trade Commission told the United States Congress that it advises against creating a Do Not E-mail Registry because such a registry would fail to reduce spam, could not be effectively enforced and could even increase spam if spammers misused it: “[t]he high value of e-mail addresses would likely make a Registry the National *Do* Spam Registry”.⁴⁴ Such concerns are highlighted by the recent theft of 92 million e-mail addresses from America Online.⁴⁵

Instead, said the FTC, anti-spam efforts should focus on e-mail authentication.⁴⁶ Groups such as Microsoft are heavily involved in this effort, and are attempting to develop new protocols to ensure that the origin of e-mails cannot be falsified.⁴⁷ But it is important, in moving forward with authentication and identification technologies, that certain rights in e-mail communication be preserved. Vigilance is required in protecting anonymity and privacy. For instance, a centralized “whitelist” of approved e-mailers should not be required, and new technologies should not interfere with consumers’ ability to use anonymous “re-mailer” programs.

4.6 New challenges: Loss of sender privacy

Recently, there have been significant developments on the spam front that may affect consumer rights. In particular, a proposal has been submitted to the Internet Engineering Task Force (IETF) for Sender ID, which would establish an industry-wide standard for e-mail authentication. The proposal incorporates recommendations from Microsoft for Caller ID and from Pobox.com for Sender Policy Framework (SPF). The purpose of Sender ID is to help verify the source of e-mail and to reduce the risk of domain spoofing and phishing.⁴⁸

Under the merged proposal, organizations will publish information about their outgoing e-mail services, such as their IP address. Sender ID will allow the receiving system to test for spoofing at the message transport level (SMTP), as well as in the message body header. Industry groups broadly favour e-mail authentication. The Anti-Spam Technical alliance, including America Online, British Telecom, Comcast, Earthlink, Microsoft, and Yahoo have recently expressed support for Sender ID.

From the consumer perspective, it remains unclear whether this approach will reduce the spam problem. While consumers clearly favour techniques that will diminish spoofing and phishing, user-identified e-mail also raises the prospect of more intrusive data collection that will lead to more aggressive commercial marketing by the private sector and more surveillance under law enforcement. Such a scheme could also impact on principles of free expression and anonymity, if senders of non-commercial messages are required to disclose their identity.⁴⁹ As the Council of Europe stated in its Declaration on Freedom of Communication on the Internet:

Council of Europe Declaration on Freedom of Communication on the Internet

Principle 7 - Anonymity

“In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and cooperating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.”

Source: Council of Europe at: <http://www.coe.int/>.

United States law also recognizes a Constitutional right to protect the privacy of identity in several contexts, including membership in political organizations, commercial protest, political speech, and even door-to-door solicitation.⁵⁰ The right of anonymity is viewed as critical component of the First Amendment.

At the very least, user-identified techniques for countering spam should comply with international data protection principles, including ones that require the minimization or elimination of the collection of personally identifiable information. User-identified e-mail, while perhaps the favoured solution of industry groups, imposes a new cost on Internet users and that is in the loss of privacy that results.

5 Conclusion

Spam remains a critical concern for the future of the Internet. It imposes a significant cost on service providers and consumers. It is already leading some to turn away from Internet-based services. If left unchecked, the problem of spam will rapidly degrade the Internet as a medium for commerce, science, and political expression.

Consumer education can help consumers identify privacy tools that may limit spam, but it remains an incomplete solution. International cooperation is critical, but spammers often evade detection. Technical solutions are also creating new problems. Filters, for example, both underblock and overblock e mail. User identification schemes, such as Sender ID, may reduce the risk of spoofing and phishing but they will also increase privacy risks for consumers as personal information will be readily obtained.

In the effort to combat spam, consumers face both challenges and challenges.

-
- ¹ TransAtlantic Consumer Dialogue, TACD, "Unsolicited Commercial Email" (2001), <http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=98>
- ² Brightmail, "Spam Percentages and Spam Categories" (June 2004), available at <http://www.brightmail.com/spamstats.html>
- ³ See Federal Trade Commission, "You've Got Spam: How to 'Can' Unwanted Email," <http://www.ftc.gov/bcp/online/pubs/online/inbox.htm>
- ⁴ *Id.*
- ⁵ See <http://spamcon.org/directories/filtered-mailboxes.shtml> (lists filters and filtering services).
- ⁶ Based on the actual experience of the author. The first message was routine spam, the second was from a political mailing list to which the author subscribes.
- ⁷ "Background Paper for the OECD Workshop on Spam," Organization for Economic Co-operation and Development's Directorate for Science, Technology and Industry, January 22, 2004, p. 26. (Originally presented to the Working Parties on Telecommunications and Information Services Policy and on Information Security and Privacy, and the Committee on Consumer Policy, during their meetings in 2003. Declassified in January 2004.) [http://www.oelis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp\(2003\)10-final](http://www.oelis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp(2003)10-final).
- ⁸ "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unsolicited commercial communications, or 'spam'," Commission of the European Communities, Brussels, January, 22, 2004, p. 27. http://www.icp.pt/streaming/spam_com_2004_28_en.pdf?categoryId=91419&contentId=154672&field=ATTACHED_FILE.
- ⁹ <http://www.cnil.fr/> (In French only).
- ¹⁰ <http://www.ftc.gov/bcp/online/edcams/spam/consumer.htm>.
- ¹¹ http://www.aca.gov.au/consumer_info/spam/consumerinformation.htm.
- ¹² <http://www.aui.es/> (In Spanish only).
- ¹³ <http://www.aui.es/> (In Spanish only).
- ¹⁴ <http://spamcon.org/>.
- ¹⁵ <http://www.spamhaus.org/>.
- ¹⁶ <http://www.antispam.org.sg/>.
- ¹⁷ http://minwon.spamcop.or.kr:5010/eng/m_3_3.jsp.
- ¹⁸ www.spamcop.or.kr.
- ¹⁹ "Communcation," *supra*, pp. 12-13.
- ²⁰ <http://www.informationcommissioner.gov.uk/eventual.aspx?id=5801>.
- ²¹ "Communication," *supra*, pp. 12-13.
- ²² See http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e.html.
- ²³ <http://www.isc.org.cn/20020417/ca226065.htm>. See Li Yuxiao, "Anti-Spam in China," presented February 26, 2004 at Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE) Conference, Kuala Lumpur, Malaysia. See also Andrew Yeh, "China Now World's Number Two Spam Recipient, After United States," Privacy and Security Law Report, Vol. 3, No. 13, March 29, 2004, p. 361.
- ²⁴ <http://www.hkispaspa.org.hk/>. See http://www.ofta.gov.hk/frameset/home_index_eng.html.
- ²⁵ http://www.ofta.gov.hk/frameset/home_index_eng.html.
- ²⁶ <http://stopspam.net.nz>. See David Harris, "A Presentation to APCAUCE on the 'State of the Nation,'" presented February 26, 2004 at Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE) Conference, Kuala Lumpur, Malaysia

-
- ²⁷ <http://ssc.sitf.org.sg/default.aspx>.
- ²⁸ <http://www.ftc.gov/secureyourserver/>; <http://www.antispam.org.sg/>. See also "FTC and Other International Agencies Join Forces to Combat Flood of Spam," Privacy and Security Law Report, Vol. 3, No. 5, March, 2, 2004, p. 113.
- ²⁹ <http://www.econsumer.gov/english/index.html>.
- ³⁰ <http://www.apcauce.org/>.
- ³¹ Mark Ward, "United Front Against Spam Urged," BBC News Online, June 8, 2004, <http://news.bbc.co.uk/1/hi/technology/3786511.stm>. See also Graeme Wearden, "Europe 'Near Agreement' on Cybercrime Fight," ZDNet UK, June 9, 2004, <http://news.zdnet.co.uk/internet/security/0,39020375,39156968,00.htm>.
- ³² John Herzfeld, "U.K. Anti-Spam Enforcement Hindered by National Boundaries, Official Says," Privacy & Security Law Report, Vol. 3, No. 18, May 3, 2004, p. 531.
- ³³ Marc Rotenberg, Testimony and Statement for the Record, Hearing on Spam (Unsolicited Commercial E-Mail), Before the Committee on Commerce, Science and Transportation, United States Senate, May 21, 2003.
- ³⁴ Letter from members of The Privacy Coalition to Members of Congress, May 13, 2003 (http://www.privacycoalition.org/spam_letter.html)
- ³⁵ "Opinion 5/2004 on Unsolicited Communications for Marketing Purposes Under Article 13 of Directive 2002/58/EC," Article 29 Data Protection Working Party, adopted on February 27, 2004. (The Data Protection Working Party was created to advise the Commission of the European Communities and bring together data protection authorities in the EU.) http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp90_en.pdf
- ³⁶ Para 1, Art. 13 of the Directive.
- ³⁷ As required by the Data Protection Directive 95/46/EC.
- ³⁸ Working Party Opinion, p. 5.
- ³⁹ *Id.*, p. 7.
- ⁴⁰ "Consumer Attitudes Regarding Unsolicited Commercial E-mail (Spam), October-December 2003," Trans Atlantic Consumer Dialogue. <http://www.tacd.org/docs/?id=225>.
- ⁴¹ Lee Rainie and Deborah Fallows, "Pew Internet Project Data Memo," March 2004, http://www.pewinternet.org/pdfs/PIP_Data_Memo_on_Spam.pdf.
- ⁴² Deborah Fallows, "Spam: How it is Hurting Email and Degrading Life on the Internet," October 22, 2003.
- ⁴³ Similar findings were made by Consumer Reports. A March report showed that 80 per cent of e-mail users had not seen any reduction of spam since CAN-SPAM went into effect. Additionally, a majority reported that opt-out links were not very effective in stopping spam. See Senate Commerce Committee hearing on CAN-SPAM, May 20, 2004, testimony of James Guest, Consumers Union President, at <http://commerce.senate.gov/hearings/witnesslist.cfm?id=1199>.
- ⁴⁴ <http://www.ftc.gov/reports/dneregistry/report.pdf>.
- ⁴⁵ Jon Swartz and Byron Acohido, "AOL Breach Gives Spam Fight a Twist," June 6, 2004, http://www.usatoday.com/money/industries/technology/2004-06-24-aol-cov_x.htm.
- ⁴⁶ "The Commission thus proposes a program to encourage the widespread adoption of email authentication standards that would help law enforcement and ISPs better identify spammers. If, after allowing the private market sufficient time to develop, test, and widely implement an authentication standard, no single standard emerges, the Commission could begin the process of convening a Federal Advisory Committee to help it determine an appropriate email authentication system that could be federally required." *Id.*, p. 7.
- ⁴⁷ Graeme Wearden, "Microsoft Double Whammy Hammers Spam," Silicon.com, June 29, 2004, <http://www.silicon.com/research/specialreports/thespamreport/0,39025001,39121737,00.htm> (discusses the proposed combination of Sender Policy Framework and Microsoft's Caller ID).

-
- ⁴⁸ “MTA Authentication Records in DNS,” June 2004, available at <http://www.ietf.org/internet-drafts/draft-ietf-marid-core-01.txt>. See “IETF Releases Anti-Spam Sender ID Internet Draft Specification,” June 25, 2004 available at <http://xml.coverpages.org/ni2004-06-25-a.html>.
- ⁴⁹ Article 10 of the European Convention on Human Rights (ECHR), enshrining the right of freedom of expression and information.
- ⁵⁰ See *NAACP v. Alabama*, 357 US 449 (1958), *Talley v. California*, 362 US 60 (1960), *McIntyre v. Ohio Election Commission*, 514 US 334 (1995), *Watchtower Bible v. Village of Stratton*, 122 S. Ct. 2080 (2002).