Combating Spam:
Policy, Technical and Industry Approaches

INTRODUCTION

Spam continues to be a significant problem for Internet users and operators, even as email filtering and blocking efforts by network operators, software vendors and Internet service providers (ISPs) more effectively stop spam before it reaches end users' mailboxes. Recent estimates by reliable organization [1, 2] nonetheless indicate that spam makes up between 70% and 80% of email traffic worldwide. Thus, spam can create a significant burden for network operators, and the problems associated with spam may be magnified in developing countries, where high volumes of incoming and outgoing spam can cause a severe drain on the limited and costly bandwidth that is available in those regions[3].

What is spam?

Even though the problem of spam has been with us since the 1990s, there is no single accepted definition. The term is widely understood and in general use, and in general the concept includes the notions that spam includes unwanted electronic communications, generally commercial in nature, and increasingly likely to be a source of malware. Attempts to freeze a definition in time are likely to be futile, because the nature of the problem changes at the same speed as the change in Internet technology and applications. For example, concerned individuals and organizations note the spread of spam to mobile technologies, as for example through SMS and MMS messages.

"Spam affects everyone involved with the Internet including, among others, network operators, ISPs, businesses, recipients and, at the most basic level, the infrastructure itself through burden that it places on the system. For that reason, fighting spam requires a multi-stakeholder approach."

What is being done to fight spam?

Spam affects everyone involved with the Internet including, among others, network operators, ISPs, businesses, recipients and, at the most basic level, the infrastructure itself through burden that it places on the system. For that reason, fighting spam requires a multi-stakeholder approach. For concrete solutions that will combat the causes and effects of spam, the coordinated efforts of stakeholders from both private and the public sectors are required, including but not limited to:

- Legislators and public regulatory authorities, including communications regulators, consumer protection agencies and others such as privacy and data protection officials;
- Criminal and civil law enforcement agencies;
- ISPs and other providers of mail services;
- Host operators -- operator groups
- Organizations responsible for developing relevant standards and best practices
  Electronic marketers
- Organizations representing Internet users
- Private sector entities dedicated to addressing issues related to spam such as those involved in spam filtering or in combating "phishing."

The cooperation of operational actors, each in their area of competence, is a critical source of knowledge for governments and others involved in anti-spam efforts. For instance, an

understanding of emerging technologies intended to curb spam is central to assessing the context and possible outcomes of domestic legislation, or negotiations held in different international meetings. At the same time, Internet users and e-commerce firms need to have a clear definition of what is prohibited (spam) and what is not (legitimate mail).

This paper is intended to provide pointers to some of the main players in the effort to fight spam and some examples of the many approaches that are being taken. Although it is necessarily incomplete, this compilation shows the range of stakeholders engaged in different initiatives, and is intended as a starting point for anyone wishing to understand the problem or to get involved in combating spam.

GOVERNMENT MEASURES AGAINST SPAM

Around the world, governments are taking measures to combat spam, although it must be said that these efforts are more common in Western, developed countries. A fairly comprehensive, if somewhat dated, source for tracking the range of anti-spam laws is available at <http://spamlinks.net/legal-laws.htm>.

National Approaches:

Several countries have enacted specific spam related legislation or developed regulatory measures. Some key examples are:

Australian Spam Act and Codes of Practice (2003)[4]: This Australian law covers email, instant messaging, SMS and MMS messages of a commercial nature. Under the Spam Act, it is illegal for unsolicited commercial electronic messages that has an Australian link if it originates or was commissioned in Australia, or originates overseas but has been sent to an address accessed in Australia. The legislation sets out penalties of up to $1.1 million a day for repeat corporate offenders. Australia has also developed regional bilateral arrangements for cooperation on countering spam with a number of countries, including Korea, Taiwan, Thailand the United Kingdom and the United States[5].

Canadian Anti-Spam Act (2010)[6]: The Canadian legislation requires that users "opt-in" to receiving spam and defines the core legal requirements of commercial email. To support enforcement of the legislation, the Canadian Radio-television and Telecommunications Commission (CRTC), the telecommunications and broadcast regulator, will host the Spam Reporting Centre (SRC). Consumers, businesses and other organizations will be able to report commercial electronic messages sent without consent to the SRC via fightspam.gc.ca once Canada's anti-spam legislation (CASL) is in force, expected to be in 2013.

European Commission e-Privacy and Electronic Communications Directive (2002)[7]: Article 13(1) requires Member States to prohibit the sending of unsolicited commercial communications by fax or e-mail or other electronic messaging systems such as SMS and MMS unless the prior consent of the addressee has been obtained (opt-in system), with some exceptions. Member States may also choose between an opt-in or an opt-out approach.

US CAN-SPAM ACT (2003)[8]: This Act defines legal conditions governing spam and provides users the right to opt-out of receiving spam. Several states also have enacted laws aiming directly or indirectly at spam[9]. Some of these have been superseded by the CAN-SPAM Act.

Other examples of national legislative approaches are: the *Singapore* Spam Control Bill[10], the *New Zealand* Unsolicited Electronic Messages Act[11], *Japan*'s anti-spam law[12]. Several other countries include measures pertaining to spam as a part of broader legislation pertaining to electronic commerce or communications in general (see for example a Microsoft Corp. survey of measures in the Asia Pacific region[13]).

In addition to legislative and regulatory measures, many governments produce educational material aimed at informing their citizens of steps they can take to protect themselves and their computers from the negative effects of spam. Examples may be found in Australia[14], Canada[15], Europe[16], Hong Kong[17], India[18] Malaysia[19], Peru[20] the United States[21], as well as many other countries

International Approaches:

"Because the Internet is essentially borderless and so not amenable to treatment exclusively in national law, governments have found it effective to band together voluntarily to develop international approaches to fighting spam."

Because the Internet is essentially borderless and so not amenable to treatment exclusively in national law, governments have found it effective to band together voluntarily to develop international approaches to fighting spam. Some examples are:

OECD Anti-Spam Toolkit (2004)[22]: The 34 countries who are members of this non-binding forum produced a toolkit that consists of a regulatory handbook tracking existing approaches and best practices, an examination of self-regulatory arrangements that have been tried, a resource centre consisting of technical and user-centric methods for self protection, as well as an inventory of existing partnerships. This resource was developed concurrently and in cooperation with:

APEC Principles for Action against Spam (2005)[23]: This statement by Communication Ministers of the 21 Asia Pacific economies was accompanied by a program of action, and a set of principles for action against spam. Implementation is to be voluntary, as in the case of the OECD toolkit, this statement was preceded by a significant amount of activity at the technical and policy level in various countries, and has led to some consistency in government approaches around the region. Outside of APEC, a number of countries in the region have signed The Seoul-Melbourne Multilateral Anti-spam Agreement [24]

The African Union, together with the *UN Economic Commission for Africa*, are preparing the Draft Convention on Cyber Legislation in Africa (2012)[25][26]. If accepted later in 2012, the convention would cover four main areas: e-transactions, cyber-security, personal data protection and combating cyber-crime, and has the goal of harmonizing e-legislation across the region.

The UN World Summit on the Information Society Tunis Action Plan (2005)[27]: Negotiated between 2002 and 2005, this global leaders' declaration calls on all stakeholders to adopt a multi-pronged approach to counter spam that includes, inter alia, consumer and business education; appropriate legislation, law-enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation.

United Nations International Telecommunication Union (ITU)[28]: Based on Resolution 50 of the World Telecommunication Standardization Assembly of 2004[29] the ITU has undertaken work in its Study Groups, conducted studies and information sharing activities to contribute to global governmental efforts to curb spam. In keeping with its telecommunication development mandate, the ITU has also provided valuable resources on dealing with spam and related threats[30], and has worked with the World Bank InfoDev program to develop a component of the ICT Regulation Toolkit addressing the problem of spam[31].

MULTI-STAKEHOLDER APPROACHES TO SPAM

London Action Plan[32]: The London Action Plan is a voluntary plan having 26 government signatories and approximately 30 industry participants. It is designed to promote international spam enforcement cooperation and address spam related problems. The Action Plan is open for participation by other interested government and public agencies, and by appropriate private sector representatives, as a way to expand the network of entities engaged in spam enforcement cooperation.

Internet Technical Community:

Several efforts have been made by the Internet technical community to combat the problem of spam. Some examples include:

Internet Engineering Task Force (IETF)[33]: The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.
Work is ongoing in the IETF community to develop recommendations to help deal with the spam situations. Examples are RFC 2502 (Anti-Spam Recommendations for SMTP MTAs)[34], RFC 6561 (Recommendations for the Remediation of Bots in ISP Networks)[35] and to provide information on methods being used by particular service providers, such as RFC 6108 (Comcast's Web Notification System Design)[36]. The IETF has also developed several technical approaches to help combating spam. One of them, DomainKeys Identified Mail (DKIM), is a method for validating a domain name identity that is associated with a message through cryptographic authentication. The protocol and operation of DKIM is documented in several IETF specifications (RFC 4686, RFC 4871, RFC 5617, RFC 5585, RFC 6376 - to name a few). Another protocol, complementary to DKIM, is a Sender Policy Framework (SPF) - an email validation system designed to prevent spam by detecting email spoofing, a common vulnerability, by verifying sender IP addresses (RFC4408, experimental). In addition, the IETF maintains an active spam discussion group that promotes information exchange on the topic. The related Internet Research Task Force maintains an Anti-Spam Research Group (ASRG)[37] that investigates tools and techniques to mitigate the sending and effects of spam. Its focus is on approaches that can be defined, deployed and used in the near term, by addressing underlying characteristics of spam.

Regional Internet Registries (RIRs): Regional organizations of the Internet technical community also support mailing lists and face to face information exchanges, such as the AfriNIC Anti-Spam discussion group, a long standing group serving the African community. Similar discussions take place in LACNIC serving the Latin American region, ARIN serving North America and the Caribbean, APNIC serving the Asia Pacific region, and in RIPE serving Europe and the Middle East. LACNIC also leads a regional project, supported by the Internet Society, that coordinates Computer Security Incident Response Teams, which have spam as one of their main working areas[38].

Industry-led Anti-Spam Organizations:

The Internet industry is also actively organized in a range of associations whose aim is combating spam. Two well-known examples are:

M3AAWG (Messaging Malware Mobile Anti Abuse Working Group, formerly MAAWG)[39]: is perhaps the leading place the electronic messaging industry comes together to work against spam, malware, denial-of-service attacks and other online exploitation. M3AAWG represents more

than one billion mailboxes and some of the largest network operators worldwide. It is the only organization addressing messaging abuse by systematically engaging all aspects of the problem, including technology, industry collaboration and public policy. M3AAWG leverages the depth and experience of its global membership to tackle abuse on existing networks and new emerging services, including mobile. It also works to educate global policy makers on the technical and operational issues related to online abuse and messaging.

*The Spamhaus Project[40]:*The Spamhaus Project is an international nonprofit organization whose mission is to track the Internet's spam operations and sources, to provide dependable real time anti-spam protection for Internet networks, to work with law enforcement agencies to identify and pursue spam gangs worldwide, and to lobby governments for effective anti-spam legislation. Spamhaus maintains a number of real time spam-blocking databases ('DNSBLs') responsible for keeping back the vast majority of spam sent out on the Internet. In addition to generating spam filter data and publishing real time blocklists, Spamhaus publishes the Register Of Known Spam Operations (ROKSO), a database collating information and evidence on the '100' known professional spam senders and spam gangs worldwide.

End-User Organizations:

In some countries, civil society and consumer groups are also active with efforts to educate users about how spam and how to protect themselves and their computer. In addition to the following examples, spamlinks.net maintains a list of international anti-spam sites[41].

“In some countries, civil society and consumer groups are also active with efforts to educate users about how spam and how to protect themselves and their computer.”

Coalition Against Unsolicited Commercial Email[42]: CAUCE is a volunteer Internet end-user advocacy organization. CAUCE has moved beyond its original mission of advocating for anti-spam laws, to a broader stance of defending the interests all users in the areas of privacy and abuse in all its forms on the Internet.

Media Smarts[43]: This Canadian not-for-profit has published guidelines aimed at users, and especially children, teens, parents and teachers. For example, one of their publications, Cyber Security: Spam, Scams, Frauds and Identity Theft, offers practical guidelines for self protection.

The North American Consumer Project on Electronic Commerce (NACPEC)[44]: NACPEC is a non-profit Mexican-based organization focusing on six areas of consumer protection in the electronic commerce space: (i) general regulatory aspects, (ii) jurisdiction, (iii) online-dispute resolution; (iv) spam; (v) spyware; and (vi) identity theft.

Anti-Spam Brazil[45]: Antispam.br is an informational website maintained by the Internet Steering Committee in Brazil, and is a source of reference materials about spam that is impartial and technically grounded. This site is committed to inform both end users and the network administrators about spam, its implications and how to protect and fight against it.

---

[1] http://www.maawg.org/email_metrics_report

[2] http://www.symanteccloud.com/globalthreats/charts/spam_monthly

[3] http://www.ictregulationtoolkit.org/en/section.2081.html

[4] http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_310321

[5] http://www.acma.gov.au/WEB/STANDARD/pc=PC_310349

[6] http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/FullText.html

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.d
20091219:EN:NOT

[8] http://www.ftc.gov/os/caselist/0723041/canspam.pdf

[9] http://www.law.cornell.edu/wex/inbox/state_anti-spam_laws

[10] http://www.parliament.gov.sg/sites/default/files/070006.pdf

[11] http://www.dia.govt.nz/services-anti-spam-index

[12] http://www.mofo.com/pubs/xpqPublicationDetail.aspx?xpST=PubDetail&pub=7794

[13] http://download.microsoft.com/documents/australia/AsiaPacific_Legislative_Analysis.pdf

[14] http://www.acma.gov.au/WEB/STANDARD/pc=PC_310294

[15] http://fightspam.gc.ca/

[16] http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm

[17] http://www.antispam.gov.hk/

[18] http://www.cert-in.org.in/securepc/index.html

[19] http://www.skmm.gov.my/FAQs/SPAM/About-Spam.aspx

[20] http://aplicaciones.indecopi.gob.pe/antispam/ley-antispam-peruana.html

[21] http://onguardonline.gov/spam

[22] http://www.oecd.org/internet/interneteconomy/oecdlaunchesanti-spamtoolkitandinvitespubliccontributions.htm

[23] http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel/annex_e.aspx

[24] http://www.acma.gov.au/webwr/_assets/main/lib100234/seoul-melbourne_mou-july_2009.pdf

[25] http://www.uneca.org/istd/cyberleg/dc.asp

[26] http://www.au.int/pages/infosoc/pages/cyber-security

[27] http://www.itu.int/wsis/outcome/vb/

[28] http://www.itu.int/osg/spu/spam/

[29] http://www.itu.int/ITU-T/wtsa/resolutions04/Res50E.pdf

[30] http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html

[31] http://www.ictregulationtoolkit.org/en/Section.3088.html

[32] http://londonactionplan.org/

[33] http://www.ietf.org/

[34] http://datatracker.ietf.org/doc/rfc2502/

[35] http://datatracker.ietf.org/doc/rfc6561/

[36] http://datatracker.ietf.org/doc/rfc6108/

[37] http://irtf.org/asrg

[38] http://www.proyectoamparo.net/

[39] http://www.maawg.org/

[40] http://www.spamhaus.org/

[41] http://spamlinks.net/antispam-int.htm

[42] http://www.cauce.org/cauce/about.html

[43] http://mediasmarts.ca/

[44] http://www.nacpec.org/en/

[45] http://www.antispam.br/