1. DEFINITION OF THE ISSUE

Introduction – unwanted communications

There is no internationally agreed definition of “unwanted communications” (digital or otherwise) which is not surprising because everyone has a different perspective as to what communications are unwanted. Furthermore, whether a communication is wanted or unwanted is often context dependent. For example, Alice may want to receive communications from her bank related to her account activity, but she may not want to receive communications from her bank about offers from third parties (e.g. travel industry). Bob may want to receive photos from his contacts on a photo sharing site, but he may not want to receive photos from strangers.

For the purposes of this document, “communications” means communications that occur via the Internet. They can be:

- one-to-one, one-to-many, many-to-many, among changing networks of association
- text, images, sound, video, location, movement, etc. (basically anything that can be encoded in binary)
- real-time, time-offset
- private, non-private, publication
- … etc.

There are many reasons why communications may be unwanted by recipients, including:

- they were not requested
- they are a nuisance
- they are considered an invasion of privacy
- the content is considered offensive
- they contain malware and/or spyware
- they risk being mislead or deceived by the communication with the potential to suffer financial loss, theft of identity information, and other harm
• they may incur direct financial costs (e.g. where Internet access is charged per MB or GB)

Recipients are not the only persons affected by unwanted communications. The unwitting sender (e.g. the owner of a device that has become part of a botnet or the owner of an account that has been hijacked or spoofed for the purposes of sending unwanted communications) may also suffer direct and indirect harm as a result. Unwanted communications also impact the intermediaries that are used to deliver and receive the communications such as Internet Service Providers (ISPs) and communication platform service providers (e.g. social media, email providers, VOIP providers, etc.).

Unwanted communications also affect the whole Internet ecosystem because they are a wasteful and often harmful use of a shared resource.

Spam

The remainder of this document focuses on unwanted email, often referred to as “spam” unless specified otherwise.

There is no universally agreed definition of spam, but definitions tend to converge around “unsolicited bulk e-mail[1]”.

One of the complaints is that:

“Messages are sent to multiple recipients who did not ask for them. The problems caused by spam are due to the combination of the unsolicited and bulk aspects; the quantity of unwanted messages swamps messaging systems and drowns out the messages that recipients do want”.

Added to this are the costs of mitigating spam that are borne by consumers, the Internet industry and society at large. Spam also risks diminishing trust in doing business.

Background: the rise of “spam”

The rise of spam follows the success of modern electronic communication. The speed with which, from circa 1995 onwards, e-mail communication, soon followed by messenger services, fax to e-mail services, Voice over IP (VoIP), mobile and smartphones, social networks and most recently mobile instant messenger applications, were adopted by a large portion of end-users is unprecedented.
Spammers simply adapt to use the available technology to reap the potential revenue presented to them.

In the first years of email, spammers used what was then the new technique of sending cheap bulk direct marketing messages. Soon spam became a nuisance for end-users. Their email inboxes filled up with unwanted advertisements, while having to spend valuable time to find the drowned out wanted email messages. Accordingly, the cost for Internet Service Providers (ISPs) grew through the rising number of complaints from customers and its demand on support centre capacity. Network operators faced the prospect of “clogged up” network capacity caused by large volumes of unwanted Internet traffic, which they had to address. A number of countries developed anti-spam laws. Industry developed technical measures against spam such as filtering, blocking and best practices through (cooperational) self-regulatory measures. Larger companies hired specialised security services. The cost of spam rose accordingly, with costs for countermeasures largely being borne by ISPs and network operators and their customers.

With the success of e-mail communications bad actors discovered the Internet on an ever faster growing scale. They started to send bulk misleading or fraudulent emails (e.g. advance fee frauds, the so called “419 scams[2]”, e-mails that suggest sending an amount of money with the promise of grand returns) and with time much worse. Such as phishing[3], fake pharmaceuticals threatening the health of people and emails containing (links to) unsolicited software (“malware”) enticing the unsuspecting end-user to click on the attachment or link and infect his device with malware. The infected device, now under the control of the spammer, is used to send more spam through this device[4]. This is commonly called a “bot” or “zombie” computer. Put together these devices were named “botnets”. Cost for mitigation rose accordingly again.

**Defining “spam”**

The EU Directive 2002/58 restricts spam to unsolicited commercial communications including e-mail, automated calls, SMS text and fax messages. The Netherlands has broadened this to include ideological and charitable electronic communications. In the EU, spam is approached from a privacy infringement point of view. The Directive only restricts the sending of spam.

The United States’ CAN/SPAM Act does not address the sending of unsolicited electronic communication and spam like the EU Directive and most other spam acts
do. It takes foremost measures against bad actors\textsuperscript{7}. The Can/SPAM Act aims at protecting consumers and only forbids commercial e-mail that is fraudulent, or was sent after the recipient requested the sender to stop.

Industry, in stopping unwanted bulk e-mails from reaching its customers, arguably takes the broadest measures possible and filters out all unwanted bulk sent e-mails as spam whether commercial or otherwise. As someone from the industry community posted to the Best Practice Forum: “I rely on the definition of Spamhaus”: "Spam is Unsolicited Bulk E-mail ("UBE"). Unsolicited means that the recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content”[8]. From comments in the group it can be concluded the internet industry does more than the law requires, especially in the U.S. where it is allowed to send direct marketing communications until someone opts-out. They presume that it is unwanted.

On average, it is possible to say that for most countries that have passed anti-spam law, unsolicited commercial electronic communications are prohibited, which is wider than just email. For the internet industry, all other unsolicited bulk e-mail is added, but non email messages are mostly not covered.

Some metrics on spam to size the problem

There is a multitude of reports available on the numbers of spam, so called spam metrics. Reports originating from different sources\textsuperscript{9}. They give strong indications of the state of spam. Unfortunately not more than that. These metrics vary strongly, for reasons that are not easy, perhaps impossible to ascertain[10]. Let us suffice to say that they all indicate that the numbers of spam sent run in the tens of billions up to over 250 billion, per day. Reports indicate that in 2014 numbers have risen sharply compared to 2013\textsuperscript{11}. In general they indicate that spam is a major threat to end users and society and that the loss of economic value through spam is estimated as enormous. Beyond this general statement it is hard to quantify the true amount of spam generated. What is important to understand when looking at these metrics, is that spam coming from a country does not necessarily have a relation to that country. It’s just sent from there. The spammer and/or the one who sent the spam is often in another country.

What is of interest to point out, is that several statistics indicate that having spam legislation makes a difference. e.g. Anti-Virus vendor Trend Micro on a daily basis...
produces a world map with data that shows, per country, the percentage of spam set off against the total number of e-mail messages[^12]. Up to a certain extent this map shows which country has anti-spam legislation in place and which country has not. The relative spam figures of most countries with spam legislation or a law are (considerably) lower. Finland is on top, a country with a strict “spam” anti-botnet, disinfection legislation and a regulator, FICORA, seeing to it that self-regulatory measures are undertaken by the ISPs[^13]. This is relevant information. The shorter a device is infected with malicious software sent in spam, the less spam can be sent from this device. Spam metrics from Finland present low figures and show how through legislation in combination with self-regulatory measures, government and industry together can have a major impact on the sending of spam within a country.

To understand what spam is used for in 2014, i.e. where the spammer’s revenue comes from, two views can be presented on spam messages from last and this year. Symantec states over 2013[^14]: that on average 18% of spam messages advertised pharmaceuticals, 73% was on adult content and dating. 1 in every 196 messages contained (a link to) unsolicited software (“malware”) trying to infect the receiving device, while 1 in 392 spam e-mails contained a phishing message, aimed at obtaining personal (usually but not necessarily financial) data. The remaining percentages are e.g. commercial e-mails and stock (price manipulation) spam. However, Trend Micro in the first half of 2014 sees a totally different division of spam e-mails. This is the top 3: malware (20%), health (16%) and commercial e-mails (11%)[^15].

To conclude. Although the value of spam metrics is relative due to the differences between the reports and the ways the data can be interpreted, in general, with some notable exceptions, spam metrics reveal the following:

1) Spam is a major issue for different stakeholders;

2) A spammer spams to make money or to obtain money that is not rightfully theirs;

3) Spam in 2014 is more violent, intrusive and malicious than circa 2000 when the first anti-spam laws were in the drafting process[^16].

4) A country ranking high often has a high number of internet connections;

5) Often there is a (corresponding) high infection rate with malware;
6) There is in general a connection between lower scores and anti-spam legislation and;

7) An active regulator/anti-spam enforcement process.

The stakeholders

The Organisation de Coopération et de Développement Economiques or Organisation for Economic Co-operation and Development (OECD) in 2006 published its anti-spam toolkit[17]. It identified several different stakeholders who each can take measures against spam. On both the individual and multi-stakeholder level, as “there is no silver bullet fighting spam”. The toolkit recognises: Governments, Users, ISPs/Network Operators, Technical community and expert organizations such as e.g. MAAWG, IETF, LAP, ITU. Without either of these stakeholders’ involvement, it is impossible to fight spam successfully[18]. Below, under Section 3, the main recommendations of the OECD Toolkit are presented.

Concluding

Spam affects many different stakeholders in different ways. From being a mere nuisance, spam grew to cause substantial costs, has led to substantial losses and threatens a person or a company’s on- and offline security. At the same time these stakeholders all have a role to play in the mitigation of spam. The fact that there is only a rough consensus on what spam is, is irrelevant. Active stakeholders operate successfully from their own definition of spam. Others could be invited to step up their efforts. Multi-stakeholder dialogue, cooperation and partnerships could be improved or invited to start.

2. REGIONAL SPECIFICITIES OBSERVED (E.G. INTERNET INDUSTRY DEVELOPMENT)

The nature and state of Internet access

The nature and volume of spam that is generated and received within a country or region is impacted by the nature and extent of Internet connectivity. Regions with previously limited connectivity might become a new source for spam and/or a new target for spammers. Often this occurs before any sort of anti-spam law is passed and implemented.

Countries with less bandwidth availability may suffer from congestion and significantly higher costs where there is major incoming and outgoing spam traffic.
**Differences in anti-spam laws**

Anti-spam laws vary in what is covered and allowed and what is not. The most common difference is opt-in vs. opt-out. Basically, an opt-in regime allows only commercial electronic communications if there is prior consent or transaction with a customer[19]. In an opt-out regime, commercial e-mails are generally allowed to be sent until a receiver asks the sender to stop. So, while commercial bulk e-mail may be regarded as “spam” by network operators and ISPs and filtered as unwanted communications, it is not necessarily prohibited by law. For example: the United States and South Africa have an opt-out regime. Most other countries have an opt-in regime[20].

**Regional differences in effectively combatting spam**

Spam lost its acute stature in many developed countries for several reasons. For example:

- Relevant industry partners have taken appropriate measures to filter out or block spam from reaching end users’ inboxes;
- There is a User education process to inform them of the steps they can take to address unsolicited email;
- Direct marketers in several countries adhere to Best Practices and self-regulatory rules[21];
- In several countries, law enforcement agencies have had some success enforcing anti-spam laws (a specific and general deterrent);
- There are also countries and network operators whose activity provide a feedback process to report spam.

Unfortunately, none of these measures however have the desired effect of stopping the most brazen of spammers[22]”.

And, countermeasures have not reached the same level of maturity in all countries. Many countries have not addressed spam in their respective legislation and for those that have, the quality of the tools e.g. enforcement, collaboration, Best Practices development available in the legislation varies greatly. This directly affects the effectiveness of a law. The same goes for agency resources to combat spam.
Also, there are great differences between countries in the way a government agency can cooperate with colleague agencies at the national, regional and international levels. Nonetheless, the London Action Plan[23] has contributed to cooperation and a cross border dialogue among the international anti-spam community[24].

*Reputation driving action*

For many industry stakeholders, spam rapidly became a reputational liability in the late 1990s and early 21st century. Spam was seen as negative. The ISP and telecommunication industries started to organise itself around the topic[25] and discussed, developed and implemented best practices to manage and prevent the receipt of spam and also the sending of spam (although the main focus initially was on the receipt).

One very common, effective technique to combat spam was blocking outgoing Port 25 traffic in residential or dynamic IP space. The advice to ISPs to block this Transmission Control Protocol (TCP) port was one of the first widely advertised measures in fighting spam[26].

The technical Internet community has also drafted proposals for techniques that prevent spam from being sent. Over the past decade and a half several solutions have been presented in the form of Requests for Comments (RFC) within the Internet Engineering Task Force[27] (“IETF”). Below, in section 3, an extensive overview is presented of some of the anti-spam solutions.

Direct marketers took it upon themselves to draft self-regulatory binding rules. e.g., the U.K. Direct Marketing Association’s code of conduct[28] assists its members to adhere to the different regulations addressing the sending of spam. On top of that it also obliges its members to operate in a transparent way and has self-regulatory measures in place to act against members who break the code of conduct in some way. As the DMA states: “The DMA Code is the code of conduct to which you and all DMA members must work, on top of all legal requirements”[29].

For developing countries it may be harder to join or participate in expert organisations like the Message Anti-Abuse Working Group, MAAWG, an industry driven association of experts or the London Action Plan, the global initiative for spam enforcement authorities on a regular basis, due to financial reasons.

*Cost of spam*
Spam imposes a cost on the Internet ecosystem and its participants from the people working on preventing measures, to education and training, and investments in protection and recovery. The way organisations and people are able respond to the challenges spam poses, is not the same around the globe.

A study\textsuperscript{[31]} published in 2008 on cost could still be relevant. It states that the largest cost of spam is the cost of employees at businesses having to wade through the spam in their respective company inboxes every day. An estimated 1,200 minutes in working time per year were lost due to spam per employee. With successful spam management and filtering techniques this issue will have lost its relevance in developed countries. With the rise of spam in developing countries in combination with the absence of (self-) regulatory measures, the issue may soon have relevance there. This is underscored by the presentation Animesh Bansriyar, an architect at Cloudmark, gave at the India Anti-Abuse Working Group\textsuperscript{[32]}.

Concluding

The challenges spam presents to society at large are huge, involving many different stakeholders, with different objectives and priorities. At face value these challenges are the same for developed nations and developing nations, i.e. spam is spam. What makes it different for developing countries is that most are at the starting phase of developing policy, education, training, the implementation of technical measures, etc., while a lack of financial opportunities pose an extra challenge for these countries to act upon spam. The positive side is that there are many good practices that can be used as a basis for implementation of future policy.

3. EXISTING POLICY MEASURES AND PRIVATE SECTOR INITIATIVES, IMPEDIMENTS

Over the past decade and a half several very different measures have been implemented or developed by different stakeholders that contribute with more or less success at mitigating spam.

Some examples appear below.

Intergovernmental action

As part of the need to understand and frame an approach the OECD created a Task Force on Spam in 2004 to address the development of an Anti-Spam Toolkit\textsuperscript{[33]} as a framework of recommended policies and measures addressing regulatory approaches,
enforcement co-operation, industry driven activities, technical solutions, education and awareness initiatives, spam measures, and international co-operation and exchange[34].

The OECD Task Force outlined several approaches to address the issue of spam:

- Creation of a spam regulation handbook – a reference guide to the different existing approaches to spam regulation to help identify loopholes and ways of improving international enforcement and cooperation;
- An examination of the self-regulatory arrangements which exist at industry, national or international levels which can be applied against spam;
- An analysis of existing and emerging technical measures against spam, including authentication technology;
- A central resource of information to educate and raise awareness of the threat of spam and how to fight it. This will include tips for users on how to protect themselves from spam and how to avoid “phishing”, when spammers use fake emails to encourage Internet users to divulge confidential financial data.

The London Action Plan (LAP)[35] was founded in 2004 with the purpose of promoting international spam enforcement cooperation. Since inception, LAP has expanded its mandate to include additional online and mobile threats, including malware, SMS spam and Do-Not-Call. LAP membership includes representatives from the government regulatory and enforcement community and interested industry members. Through annual meetings and bimonthly teleconferences, members stay connected and share information that is critical for any organization engaged in anti-spam regulation and enforcement.

In 2005, the APEC Telecommunications and Information Ministerial Meeting issued “APEC Principles for Action against Spam”[36].

In 2014, the 23rd Ordinary Session of the Summit of the African Union[37] adopted the African Union Convention on Cyberspace Security and Protection of Personal Data, which includes provisions addressing advertising by electronic means (including by electronic email)[38].

The International Telecommunications Union (ITU) Development Sector Study Group 2[39] focuses on ICT applications, cyber security, emergency telecommunications, and climate-change adaptation. There are two areas where the ITU-D Study Group 2 will work on the issues of spam. Question 3, Access to cloud
computing: challenges and opportunities for developing countries, including security issues such as spam and Question 6, work on Best Practices for Consumer information, protection and rights: Laws, regulation, economic bases, consumer networks, which includes spam.

**Governmental action at the national level**

Several countries have adopted specific anti-spam legislation or incorporated provisions regarding spam in another law. According to Wikipedia 34 countries, the EU and Hong Kong address spam in their law. However, Chinese Taipei, Lithuania, Estonia and a few other EU countries are also known to have implemented anti-spam legislation. The list may therefore not be complete. However, there are still many jurisdictions that do not make spam illegal.

An anti-spam law often creates a specialised regulatory agency that is given the task of enforcing the law. This could involve negotiation with spammers to cease, enforcement, as well as tools for investigation (e.g. the ability to obtain evidence), the ability to disrupt the operation of spammers and collaboration with law enforcement where fraudulent activities have occurred as the result of spam.

There is considerable variation in the organisations that are tasked with enforcement and sometimes there is more than one agency within a country that has responsibility. For example: consumer protection agencies, consumer ombudsmen, privacy regulators, telecommunication market regulators, trade regulators, government-led CERTs, ministries, competition regulators, and others.

There appear to be a number of impediments to successful cooperation across organisations. The first is the strength or weakness of the enforcement tools that the organisation can work with on the basis of the law. For example, some agencies have none or far too little tools to investigate beyond a spammer who makes himself known in the communication. Most spammers do not do this. Cross border, jurisdictional issues are often not well addressed in connection to the sharing of data. Organisations find it hard to meet each other regularly. Privacy laws (are perceived to) stand in the way of successful investigations and data sharing, e.g. an IP address is seen as personal data in many countries, which makes exchanging it between organisations difficult. A second major challenge is the attribution of spam. e.g. a clear difference between the sender of spam and his contracting partner is not always made, making it hard for agencies to successfully conclude an investigation that addresses all involved in a spam case. I.e. The sender (“the button pusher), the
contracting party and consciously facilitating parties. A third challenge involving cross border issues is that some spam laws do not define territoriality in such a way that spam is forbidden when it comes from one country into another or leaves one country for another. The case of the Dutch Independent Post and Telecommunication Authority[42] (OPTA) against “Dollarrevenue”, although a malware spreading case it has implications for spam enforcement, ended with the fine being annulled in court just because of territorial issues[43]. Not having a level playing field between agencies is a major impediment to fighting spam with a chance at success[44]. On top of this, several agencies found that with the initial success of fighting “the low hanging fruit” of spammers, now that the real cases have to be dealt with, there is no one at policy level to address. Interest has waned, as spam is not seen as a problem anymore, which is also due to the successful measures of industry. There are several impediments with the first generation spam laws. They do not stand up to the current challenges at hand.

Governments also assist in setting up public-private partnerships whose goal is to drive down spam volumes (e.g. via national support centres[45] in countries like Australia, Belgium, Germany, South Korea, Japan, The Netherlands and Croatia where end users are alerted and assisted in disinfecting their malware infected devices). Each disinfected device stops sending spam messages. Another example is Signal Spam in France, a national reporting centre for spam on a public – private basis[46].

Governments often play a role in leading or facilitating awareness campaigns directed at end-users and SMEs. It is hard to assess real effectiveness of these campaigns because there is no obvious way to measure how this activity changes behaviour (e.g. steps taken to prevent a device becoming a spam source; or steps taken to deal with spam that is received), however, it may be possible to comparatively estimate spam volumes within a community before and after such campaigns. Financial institutions are also often active in anti-phishing campaigns: the focus there is on helping customers recognise a misleading or fraudulent email and/or message.

Perhaps the hardest challenge is to make a long-lasting impact on the well-resourced criminal motivated spam, particularly where the conduct is undertaken across multiple borders. The LAP/MAAWG study ‘Best Practices to Address Online and Mobile Threats’ not only provides an extensive overview of the threats that have arisen since the publication of the OECD’s anti-spam toolkit, it also clearly presents the challenges law enforcement faces fighting spammers across borders[47].
End users

There seems to be a need for greater focus on ensuring digital literacy: Internet use comes with risks as well as benefits. End users would benefit from a better understanding of the value to themselves and other Internet users of using spam, privacy and security tools, as well as an understanding of the impact that their inaction might have.

Debates on Internet safety sometimes focus on the need for education of end users. The fact that there are no rules for Internet users is one of the impediments to addressing spam successfully[48]. However, the vast majority of spam is deliberately generated by a small number of malicious actors in circumstances where such conduct is often illegal in many jurisdictions. So in that sense, there are already rules.

Internet industry

The Internet industry has implemented a variety of technical measures designed to prevent spam from reaching the end user’s inbox. At the network layer, as well as at the ISP, techniques are in place to check email traffic against a set of characteristics that are indicative of spam. This technique is generally called “filtering”. Common uses for mail filters include organizing incoming email and removal of spam and computer viruses[49].

Constant refinement of these techniques is needed to endeavour to make sure that the number of wanted messages that do reach a customer is as low as possible.

However, with the introduction of email filter techniques, spammers became more inventive. To bypass filters they started sending attachments containing spam messages with or without malicious links or software, PDFs, pictures containing spam, etc. Consequently, network operators, ISPs and the technical community have to stay abreast of these innovations and adapt to them as quickly as possible.

The number of filtering techniques and other anti-spam measures in use around the world is extremely long. There is a good overview on Wikipedia, which gives a basic description of anti-spam techniques including filtering techniques[50]. Discussions within the Best Practice Forum also made it clear that reputation of brand and spam filtering are closely connected. An underperforming ISP, may receive a bad reputation among its peers and come to find it more difficult to send email messages outside its network.
A service that the industry relies on to be able to filter is “blocklisting”[51]. IP addresses that are identified as a source of spam, e.g. by anti-virus vendors or organisations like Spamhaus, are put on a list as a known spam IP address. This list is called a “blocklist”. Blocklisted IP addresses are effectively rendered unusable, as most organisations on the Internet will block or filter out all traffic coming from that address. Blocklists from organisations with a good reputation are followed instantly. Part of this reputation is having procedures in place to deal with addresses that have been blocked unfairly or known as false positives.

ISPs, network operators and the direct marketing industry have found each other in MAAWG, the Message Anti-Abuse Working Group. The group aims “to work collaboratively to produce experience driven, practically orientated guidance for ISPs, legitimate email senders and others in the community to ensure that good mail gets delivered and bad mail (spam) gets rejected.” From being an American centric organisation in 2004, MAAWG branched out to Europe first and currently has set up an Indian and an African chapter.

In general, among industry there is a large level of trust in plain view, through the way network operators and ISPs cooperate and work together on solutions for the common good in combatting spam. If there are areas in which this is not the case or insufficiently so, it may be of interest to understand the reasons behind less trust and to see whether this can in any way be resolved.

An entirely different way is the approach of Microsoft. It actively fights spam reaching its customers’ inboxes, i.e. Hotmail accounts, by taking down spam that contains malware and botnets in combination with civil action[52].

Technical internet 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)[53]*: 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)[54], RFC 6561 (Recommendations for the Remediation of Bots in ISP
Networks)\[55\] and to provide information on methods being used by particular service providers, such as RFC 6108 (Comcast's Web Notification System Design)\[56\]. The IETF has also developed several technical approaches to help combating spam. One of them, DomainKeys Identified Mail (DKIM)\[57\], 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)\[58\] - 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)\[59\] 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. A simple, effective, and straightforward method for using ingress traffic filtering to prohibit more invasive security threats such as DDoS\[60\] attacks which use forged (also called “spoofing”) IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point, is BCP 38\[61\].

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\[62\].

Direct Marketing Community

In several countries with an existing anti-spam law, direct marketers have adopted self-regulatory measures that aim to ensure that what they send on behalf of their customers is sent in accordance with the relevant anti-spam law. These codes of conduct can e.g. aim at more transparency and identify steps against offending members.
These examples of Best Practices are freely available from the direct marketing organizations and can be adopted by any organisation who wishes to do so[63].

Working together with the ISPs, e.g. MAAWG, best practices, operational tools and agreements can be arrived at that allow direct marketers to send legitimate bulk e-mail which will arrive at the intended destination[64].

Governments at national or regional levels could stimulate a process like this as a part of their anti-spam strategy.

Bad actors are not stopped this way, if there are no other measures available.

Spam and reputation have become closely linked. As was discussed in the Best Practice Forum: “No business wants to have their name all over the papers, labelling them as a spammer”. Spam is or will be seen as something negative, when action upon, not to be associated with as a company[65].

*Spam activists*

In several countries there are individuals and private organisations who collect data on spam or phishing and publish the results on websites. Some have become sources of influence, like the Spamhaus Project[66], CAUCE[67] (the Coalition Against Unsolicited Commercial Email) and the Anti-Phishing Working Group[68], and contribute to international debates against spam. They are considered as authorities whose input and knowledge is recognised and valued.

It is important for countries contemplating developing and introducing anti-spam measures to identify expert people or organisations like these in their respective countries, as they are most likely to be a good source on spam activities.

*Summary of possible solutions*

In this section a wide range of (proposed) solutions is to be presented. The Best Practice Forum on spam is in the process of compiling this list, which will be added after further dialogue.

**4. WHAT WORKED WELL, IDENTIFYING COMMON EFFECTIVE PRACTICES**

From the above, taking into account the impediments mentioned and challenges identified, several common effective practices or processes can be identified.
**Government leadership**

Governments by taking the lead in facilitating anti-spam discussions assist industry in focusing on solutions and self-regulatory measures. An anti-spam law with a minimal hint at enforcement drives away most, if not all commercial spammers within a limited time frame. An agency with the right investigative and enforcement tools is able to: notify commercial providers that they are breaking the law, fine most persistent common spammers; seriously frustrate most spammers active within their own country through disruptive measures and; incidentally have one fined in another country through cooperation with colleagues in other anti-spam agency[69].

**Industry leadership**

The technical measures that the internet industry have taken upon themselves to use to manage their network such as filter e-mail traffic have proven themselves extremely successful.

The process that the IETF (and MAAWG) has in place leads to internet standards and best practices and identifies tools and operational processes that work well when used within the organisation. These are developed by many internet engineering experts who come together to define issues and work on solutions on a voluntary basis.

Dedicated spam and consumer activists can be a great source of knowledge for governments, agencies and industry.

**5. UNINTENDED CONSEQUENCES OF POLICY INTERVENTIONS, GOOD AND BAD**

**Potential retaliatory action**

Entities which take action against spammers, whether voluntarily or in accordance with policy and/or law), may inadvertently expose themselves to malicious retaliatory action. One such example was the March 2013 distributed denial of service (DDoS) attack against Spamhaus when CyberBunker was added to a Spamhaus blacklist[70] and their email messages were then blocked on most ISP networks.

**Potential impact on freedom of expression and access to information**

Spam filtering is never 100% effective. It is prone to over-blocking and under-blocking email and IP addresses. There is the risk that wanted communications are inadvertently blocked or restricted, with consequent implications for freedom of
expression. While some (malicious) e-mail may still get through. Also, there may be a temptation to use such technology for censorship purposes.

**Potential impact on privacy**

While policy interventions to address spam may have the best intentions, they may have the unintended effect of interfering with users’ rights and expectations of privacy. In considering this issue, it is also important to understand that collection and handling of data, communications data, and other meta data could adversely affect an individual’s privacy.

**Tragedy of the commons**

In some cases, there may be challenges associated with deploying solutions to prevent or mitigate spam since there may be no identifiable immediate harm to the relevant actors or their assets. At the same time, neglecting it leaves others exposed and leads to the decrease in overall trust and security of the ecosystem (a “tragedy of the commons”).

A challenge in developing policy solutions for the Internet ecosystem is overcoming the “tragedy of the commons”. Effectively addressing spam requires an appreciation that action (or inaction) by one actor can have implications for the whole ecosystem.

**Designing and implementing solutions**

The design and implementation of solutions to address spam should be undertaken with consideration as to the potential effect they might have on: the development, use and evolution of the Internet; economic and social well-being; fundamental rights and values such as privacy; the impact on innovation and cross-border trade; etc. They should be evidence-based, and draw upon the interests and expertise of all relevant stakeholders.

6. **UNRESOLVED ISSUES WHERE FURTHER MULTI-STAKEHOLDER COOPERATION IS NEEDED**

There are several unresolved issues that have been identified. These will also be presented in section 8 of this document.

Addressing spam will likely always need further multi-stakeholder cooperation as the communication landscape is constantly changing. What is today a popular means of communicating via the Internet may become less so tomorrow, and new means of
communicating may emerge. Malicious actors are continually evolving their strategy and attack vectors to leverage these new applications to perpetrate malicious and fraudulent activities.

Here are some specific areas that may merit from further multi-stakeholder discussion and collaboration:

- How to help application and service providers effectively implement technical anti-spam measures;
- How to defend and recover against retaliation by malicious actors;
- How to empower users to help contribute to specific and overall mitigation of unwanted communications;
- How to fairly and equitably share the costs and benefits from mitigating against unwanted communications, particularly where such activities are transnational;
- How and where to discuss development and implementation of internet standards and best practices that assist in effectively mitigating the volume of spam;
- How to ensure that Internet resources, e.g. IP addresses and Domain Names, are not abused by spammers;
- Creating a competitive environment and level playing field for application and service providers;
- How to ensure respect of individuals’ rights and expectations of privacy while mitigating against unsolicited communications;
- Improving cross-jurisdictional technical and legal mitigation against unsolicited communications (including law enforcement);
- Impediments to effective development and implementation of anti-spam policy;
- How to engage producers of the latest generation of products that go online, “the Internet of Things”) and debate Security by Design solutions to prevent further spam volumes[71].
- Trust is one of the most elementary prerequisites for organisations to cooperate and share data when fighting spam across multiple communities. Where a lack of trust is apparent, it is important to find out the reasons behind this lack of trust and see whether this can in any way be resolved through a multi-stakeholder collaborative process.
In closing, at the WCIT-12, the following treaty text was drafted and agreed by some Member States regarding spam:

“Member States should cooperate to take actions to counter spam, including through 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”[72].

Another ITU document provides advice on how to draft an effective anti-spam law. It presents several examples of what worked and what did not work in the past. It also addresses several topics, which were identified as an impediment to successful enforcement. There is a clear advice to draft a new generation of spam laws that go “beyond mere sentiment to real action”[73].

These two items in short sum up the challenges mentioned above and once distilled into the most elementary wording, provide an insight into a way forward for this group: The need for action across a wide range of actors.

7. **INSIGHTS GAINED AS A RESULT OF THE EXPERIENCE**

Collaboration is an essential component of effective mitigation against unwanted communications.

“People are what ultimately hold the Internet together. The Internet’s development has been based on voluntary cooperation and collaboration … and that is still one of the essential factors for its prosperity and potential.”[74]

The utility of solutions to address unwanted communications is greatly dependent on the actions of many parties and their willingness to voluntarily support others within the Internet ecosystem.

There is no “silver bullet” and there will always be some level of unsolicited communications. It is important, therefore, that solutions focus on prevention or interception before they reach the intended recipients. Efforts should also concentrate on how to make the Internet ecosystem more resilient to such threats and how to help recipients address unsolicited communications.

In the above it was made clear that spam affects many different stakeholders in different ways. Spam causes substantial costs, has led to substantial losses and can threaten a persons or company’s on- and offline security. Different stakeholders
address the effects, in different ways. Sometimes through regulation, often through industry developed self-regulatory processes that have proven themselves successful. It is also possible to identify areas where stakeholders could improve their efforts or be invited to join the debate and asked to join actions to make the ecosystem as a whole more resilient.

One item to note is that there is no substantial overview of good practices across communities, regions or globally.

It is also important to appreciate that while malicious actors will exploit any opportunity, the Internet is neither the origin nor the cause of the malicious activity.

Lessons learned from the enforcement side of spam is that when given even the lightest of enforcement tools, an agency has successes to celebrate. However, where the malicious and fraudulent professional spammer is concerned most anti-spam laws fail. Challenges around international cooperation, data sharing, territoriality and jurisdiction need to be reviewed and addressed (again).

What also became clear is that now that anti-spam agencies and industry face their biggest challenge concerning spam, the interest of governments in the topic in developed countries seems to have waned considerably. However this expertise in addressing the problem of spam is important to share with broader communities who are just starting the journey of what needs to be done to address their problem with spam, for which expert resources and capacity building will need to be made available.

Reporting from emerging economies indicate that they are now facing commercial spam in fast growing numbers for the first time.

8. PROPOSED STEPS FOR FURTHER MULTI-STAKEHOLDER DIALOGUE

Further multi-stakeholder dialogue in this Best Practice Forum could focus on:

1. **Common understanding of the problem.** The more aligned stakeholders are with regard to the problems, their severity and the priority of their resolution, the more focused the dialogue is, and the more coherent various efforts aimed at mitigating unwanted communications will be.

2. **Common understanding of solutions.** The challenge here is that there is a whole array of possible solutions (technical, policy, economic, social) and
each of them solves only part, or one set of the problems at a particular point in time. It is important to understand that there is no “silver bullet”, but rather, evolving building blocks that can be used in constructing many solutions.

3. **Understanding of common and individual costs/benefits.** The technology, policy, economic and social building blocks vary in the costs and the benefits they bring individually and to the common good of the global Internet. Understanding these factors and how they are aligned with the needs of governments, Internet users, the business objectives of network operators and other stakeholders is crucial for sustained improvements in addressing unsolicited communications.

4. **Ability to assess risks.** Adequate selection of tools and approaches is dependent on the ability to properly assess risks, including risks to the whole Internet ecosystem. This requires agreement on metrics and factual data and trends associated with them. This data is also important for the measurement of the effect of such tools once they are deployed and to monitor the changing dynamics of the environment.

5. **Identifying good practices.** A good overview of good or common practices within communities involved in combatting spam seems absent or at least are unfamiliar between communities. To identify and/or make an inventory of these practices and share them with other stakeholders who have a need for this, is useful in developing multi-stakeholder approaches. These future overviews or lists could also be of added value to those starting work to address spam in developing countries.

6. **The difference between the developing and developed world.** It is important to understand that there is a difference in the challenge they face. The developing world still has to find its way in mitigating spam at its most basic level. The developed world faces the challenge of dealing with professional, mostly malicious spammers that are active from or (ab)using resources in multiple jurisdictions.

---

**Footnotes**


[2] The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud.
Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.”
http://en.wikipedia.org/wiki/Phishing

There are other forms of malware that are installed, aimed e.g. at direct financial gain, storage of illegal content, espionage, etc. Like botnets are also used for other purposes, e.g. denial of service attacks, extortion, etc.


See e.g. Sections 2.1.2 and 2.a.7.

http://www.spamhaus.org/consumer/definition/. The Spamhaus Project is an international organisation founded to track email spammers and spam-related activity

Examples are threat reports by anti-virus vendors, e.g. Symantec, Sophos, Trend Micro, Kaspersky, etc. Statistics provided by Cisco, Spamhaus and others and reports from companies like Microsoft.

However, it is important to keep in mind when examining spam metrics from companies, that gin revenue from selling solutions to combat spam may have an incentive to inflate the seriousness of the issue.

Roughly spam constitutes 85% of all e-mail traffic.


[16] The ITU paper ‘Countering spam: How to craft an effective anti-spam law’ states that “the first generation of anti-spam laws has been an unqualified failure”. This document presents facts to show that this is not necessarily true for unsolicited commercial e-mail.


[18] This is only one example. There are other organisations that can be noted. The Internet Society publication ‘Combating spam. Policy, Technical and Industry Approaches’ gives an extensive overview of other global, regional, national and sectorial initiatives.

[19] This is called a “soft opt-in”. A hard opt-in” only allows direct consent.

[20] This difference can be explained by just how successful the lobby of a DMA is.

[21] These are discussed more in-depth below under section 3.


[23] Londonactionplan.org

[24] Also look at ‘ITU Discussion paper. How to craft an effective anti-spam law’

[25] E.g. The Messaging Anti-Abuse Working Group, MAAWG (Now called M3AAWG: Message, Malware, Mobile) and Direct Marketing Associations in different countries


[29] Idem, page 1

[30] Both organisations are open by the way to public-private cooperation and knowledge sharing and meet on a regular basis.


[37] The BPF group strives to present more regional initiatives in the near future.


[40] http://en.wikipedia.org/wiki/Email_spam_legislation_by_country (accessed 18 August 2014). This number is not correct as several EU countries are missing from this list. If we add individual states in e.g. the U.S. and Germany the figure is about double. See also: ‘ITU Discussion paper. How to craft an effective anti-spam law’. Its footnote 1 refers to www.spamlaws.com. The accuracy must also be contested, as it e.g. still mentions “Yugoslavia”. LAP membership is also not accurate, as not all countries or enforcement agencies are members.

[41] In Germany e.g. it is the ISP association eco that enforces spam through civil law suits. See for the difference in anti-spam agencies
http://londonactionplan.org/members/
[42] OPTA, now part of the Authority Consumers and Markets, was the telecommunication and post regulatory authority and as such responsible for enforcing unsolicited electronic communications and malware.

[43]

[44] National Cyber Crime and Online Threat Analyses Centres. A study into national and international cooperation (De Natris Consult, Leiderdorp 2012)


[48] See e.g. a debate around “Internet driver’s licenses”.
http://www.govtech.com/security/Drivers-License-for-the-Internet.html or http://business.time.com/2010/01/30/drivers-licenses-for-the-internet/. On the same level are debates to charge users per e-mail: http://www.geek.com/news/charging-for-e-mail-will-stop-spam-551697/


[51] The term “blacklisting” is used also. The terms are synonymous.


DomainKeys Identified Mailtxt is “an email validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain is authorized by that domain's administrators”. http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

Sender Policy Framework, whereby Administrative Management Domains (ADMDs) can explicitly authorize the hosts that are allowed to use their domain names, and a receiving host can check such authorization, RFC 7208. See: http://tools.ietf.org/html/rfc7208

https://www.ietf.org/proceedings/56/asrg.htm. Note: The working group has been concluded.

“A distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users … by temporarily or indefinitely interrupt or suspend services of a host connected to the Internet”. Wikipedia, http://en.wikipedia.org/wiki/Denial-of-service_attack

http://tools.ietf.org/html/bcp38


A new technique that may grow into a best practice is DMARC (Domain-based Message Authentication, Reporting & Conformance), see: http://dmarc.org


On the same level, spam can impact the reputation of a whole country. E.g. Nigeria, because it is closely identified with the “419 scams” or “Nigerian scams”. See footnote 2.

http://www.spamhaus.org/

http://www.cauce.org/

http://www.antiphishing.org

Most notable is the HerbalKing case, a cooperation between the Australian ACMA, New Zealand’s Ministry of Internal Affairs and the FTC from the U.S., with
data shared by several other agencies. Since 2008 there has been no other international cooperation spam case. Only assistance in national cases.

[70] https://en.wikipedia.org/wiki/The_Spamhaus_Project#CyberBunker_dispute_and/DDoS_attack

[71] The first sightings of TVs, pacemakers, cars that were hacked and controlled remotely have been reported. This could lead to another increase of spam volumes.


[73] ITU Discussion paper. How to craft an effective anti-spam law