Internet Governance Forum (IGF) 2014

Best Practice Forum on Regulation and Mitigation of Unsolicited Communications (e.g. "spam")

Executive Summary

There was a general recognition that many stakeholders are involved in the fight against unsolicited electronic communications and are successful in their own way. The Best Practice Forum provided valuable insights and identified a host of topics that need further discussion, combined into 11 next steps. These are extensively presented in the main body of the report.

While the title defined by the Multistakeholder Advisory Group (MAG) had used the term "unwanted communications", the experts involved in the discussions agreed to change this to "unsolicited communications". The reason for this change was that "unwanted" could give rise to too loose interpretations and could be (mis)used for political reasons and for clamping down on freedom of expression. The term unsolicited communications, ideally, should capture all forms of bulk electronic communications and, in addition to "traditional spam", include phishing, fraud and scams, ddos attacks, the fight against botnets and the understanding and possible disruption of the spam business case.

While there was a generally held view that spam should be mitigated, there was one strong dissenting opinion expressing the fear that spam restrictions might have a negative impact on freedom of expression and privacy.

Major findings

All experts involved realize that there is no silver bullet fighting spam. Many and very different stakeholders play important roles, including end users, organizers of awareness campaigns etc. The Best Practice Forum mainly focused on self-regulatory measures of the Internet industry, legislation by governments, enforcement bodies and finally introduced the option of pro-active measures. What emerged from the discussions is that most measures are taken in isolation of other stakeholders, instead of seeing each measure as a stepping stone.

It is important to understand that spam is fought primarily at industry level. Internet companies and Internet Service Providers (ISPs) filter traffic on what they expect their customers to perceive as spam or "unwanted" (the term industry uses) communications and to prevent them from harm. Traffic is filtered on content of messages and on the basis of IP blocklists provided by trusted parties, like e.g. Spamhaus. They filter much more than traditional spam, i.e. unsolicited commercial electronic communications (the legal phrase) and include phishing, fraud and any other sort of mass mailing with criminal intent, but do not filter unsolicited fax, do not call, non-bulk messages, etc., which anti-spam laws often include.

Self-regulatory measures are reflected in best practice guidelines, Internet standards and best practices and agreed upon measures that industry bodies in the ISP (M^3AAWG), mobile (GSMA), technical Internet (IETF) and direct marketing communities (DMA's) published over the years and in general adhere to. However, self-regulation has its limits and doesn't deter "the real spammers".

The mitigation of spam is a continuous, extremely innovative battle between spammer and spam filter techniques, which comes at great effort, resources and costs for all involved in this effort. There is no business case in mitigation and hardly anybody is prepared to pay for it.

Because filtering spam is so successful, most people consider that the spam problem has been solved. The Best Practice Forum revealed that this assumption is over optimistic if not downright mistaken. The point was also made that governments have lost interest in solving the spam problem, perhaps due to the successes of filtering methods.

Spam laws are largely missing around the world and where they are in place there is only a limited number of countries with successes in enforcement. These laws often use the wording "unsolicited electronic communication", in a restricting way. Spam laws differ strongly from each other and despite that harmonization is unlikely, governments are invited to reassess their spam laws and their effectivity. However, it was noted that governments were largely absent in the Best Practice Forum discussions.

Most efforts to fight spam rely on voluntary actions and cooperation. At the basis of all voluntary cooperation lies trust. This does not come easy. Then there are jurisdictional and legal issues. Spam does not respect national borders, whereas all entities fighting spam are restricted by borders. Furthermore, privacy sensitive data are involved. Data need to be exchanged, often between private and public entities in order to mitigate a spam or bot case. These are serious issues that need further dialogue and also include stakeholder groups which are currently absent from the discussions.

The Best Practice Forum revealed that the measures different stakeholders take are often conceived in isolation and not always complementary, nor are they conceived to be complementary to other measures. Therefore, they fail to reach their full potential, as they do not play on each other's strengths. This main finding led to what arguably could be called the ultimate question this forum produced: **How can all stakeholders voluntarily assist one another, by strengthening their own and others' resolve, while remaining innovative and commercially viable?**

Suggestions for future work

The Best Practice Forum explored various areas for future work.

a. It identified the different layers where spam is or ought to be fought, such as users, industry, Internet engineers, (software) manufacturers and vendors, hardware manufacturers, mobile application developers, the financial sector, governments, law enforcement and concluded that each layer has its own role, need for knowledge, responsibilities, counter measures and level of (potential) successes. It was noted that currently fighting spam is not (always) happening in all these layers and several stakeholder groups are missing in the dialogue this far, while some always have been missing to date. It would therefore be helpful **bringing all the missing stakeholder groups together and encourage them to fight spam in all these layers, while finding ways to cooperate outside their respective layers.**

b. It was recognized that there are successful self-regulatory and legislative measures in place and best or good practices for the world to build upon. However, the view was also held that "self-regulation cannot stop persistent spammers". It was noted that spammers are usually in it for the money. They have their own economy, services, tools and channels. **The following questions therefore need to be answered: In what way can further knowledge of the spam business case contribute to the mitigation of the problem? What do stakeholders need to get involved in this assessment and following actions?**

c. Furthermore, **more input is needed from developing nations** as to better understand their problems and needs in order to address mitigation there in a better way.

d. The questions below emerged as being at the core of most topics that have been brought forward for further dialogue, such as:

- What is spam in 2014?
- Who needs to join the dialogue?
- Can a swifter implementation of Internet standards and best practices bring down spam volumes?
- Do spam laws impede on privacy and freedom of speech?
- What is needed to bring about further cooperation between different stakeholders?
- How to assist the developing world?

The Best Practice Forum in a fairly short period of time has been able to come up with defining questions, but lacked the time to search for answers or solutions.

The discussions also revealed that this issue is extremely complex, which makes it hard to agree on the basic underlying assumptions and definitions. Explanations for these difficulties are found in the differences in approach, the measures taken and starting points for spam mitigation of the respective stakeholder groups.

Unsolicited communications are fought in different ways, with different forms of success, but all efforts so far have failed to deter spammers in a decisive way. However, addressing the proposed next steps in a multistakeholder environment may lead to common understanding and to building trust among all actors, finding ways of cooperation that are innovative, heightening the defence line considerably and making spam less attractive to be involved in. Most measures discussed in the report appear to be complementary stepping stones. The challenge lies in making them truly complementary. The IGF would seem to be the ideal place to pursue this dialogue and take it a step further.

Report

In the past months this Best Practice Forum (BPF) has discussed the issue of unsolicited communications from many different angles. This paper is the outcome document of this discussions that were held up to October 2014. The debate that unfolded between the participants ranged wide and touched upon fundamental issues in many and very different ways. This outcome document cannot be seen in any way as a final document. There are many questions left to answer, topics to address and other expert stakeholders to involve. It is best seen as a starting point for further debate and discussions in 2015, working towards presenting additional outcomes at the Internet Governance Forum (IGF) 2015 in Brazil.

1. Definition of the issue

This document starts out from the premise that there is no silver bullet. Many different stakeholders are involved in the fight against unsolicited communications. Whether from a commercial, economic, idealistic, awareness raising, regulatory, security or legal perspective, all contribute in their own, valued way. In fact, this document is proof of successes by all stakeholders, but also of many challenges ahead as well as suggestions for potential future collaboration between these stakeholders. Comments to the first draft indicated that having the word regulation, as part of the title of this Forum seemed to stress that regulation is the primary goal for the output of this group. This is not the case. Still, regulation is a large part at the beginning of this report. This is only so to reflect on the debate that ensued around defining the issue at hand and especially the one around the word "unsolicited", which is a legal term introduced in most anti-spam laws. This discussion helps to underscore the differences at the starting point of action for and between different stakeholders. There are many successful self-regulatory, commercial and idealistic measures in place, which are presented below, but first this Forum needs to present the first decision it arrived at.

a. Introduction – unwanted or unsolicited communications?

This Best Practice Forum reached consensus on changing the title of this Forum to 'Regulation and mitigation of unsolicited communications (e.g. "spam")'. It was determined by the group that the term "unwanted" can give rise to subjective interpretations and allow for potential impediments on free speech.

The Forum also reached consensus to use the term unsolicited communications in the context of its work going forward. Although it is important to note that, from everyday practice, industry mitigates spam based on the premise of email that has been deemed unwanted or not asked for by end users. The group will continue to review the use of terminology to ensure that there is a clear understanding by participants from different backgrounds to minimize confusion with the term "unsolicited" over the use of "unwanted".

The term "unsolicited communications" stems from legal text and is defined in many anti-spam laws around the world. The range of what has been identified as an unsolicited communication can vary per country, based on a county's rules and social conditions. Whether more modern electronic communications as e.g. social media, Bluetooth messages, SMS, etc. fall under the local definition can also vary according to a county's approach taken for their anti-spam law and the formal explanation behind it. In short, the local law determines what is spam from a legal point of view and what is not. In-depth comparisons of individual laws falls outside of the scope of this forum, but may be an issue to pursue further in the future, as best practices and approaches can be derived from this information. There are also examples where there are no specific laws in place, however the government in partnership with local industry[1] have developed enforceable anti-spam arrangements that support consumer protection[2] legislation.

Anti-spam legislation contains many specific requirements; each country with legislation determines the best approach and set of compliance requirements that define the ways and means in which legitimate electronic mail can be exchanged. Within each law there is a process to establish "consent". Most, although not all, anti-spam laws contain some procedure to define this process. Currently there are two designations: opt-out and opt-in. Opt-out is when the receiver of the message formally notifies the sender that they no longer wish to receive messages from them (opted-out). If the receiver of the message has given his consent (opted-in), the sender is allowed to send a message to this end user. Another example is that some laws allow messages to be sent when there is an established relationship between the sender and the end user, i.e. there is a customer relationship. As a standard, all other messages, as captured by the law, become unsolicited. It is important to note that there are many best practices that have been developed around the world regarding opt-in and opt-out to ensure that users have the ability to control the communications they receive.

For the purposes of this document, "electronic 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.

There are many reasons why communications are (perceived as) unsolicited, including:

- They are a nuisance;
- They are considered an invasion of privacy;
- The content is considered offensive;
- The messages contain embedded malware and/or spyware;
- The message aims to mislead or deceive, with the potential to cause financial loss, theft of identity information, and cause other harm;
- The message may inflict direct financial costs (e.g. where Internet access is charged per MB or GB).

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

[2] http://www.fcc.gov/guides/spam-unwanted-text-messages-and-email

Another description comes from the East West Institute and the Internet Society of China cybersecurity study 'Fighting Spam to Build Trust'[3]. The report presents four essential attributes of spam as being:

- uninvited by the recipient;
- high in volume;
- distributed widely;
- an electronic message in any form.

Recipients are not the only persons affected by spam. There is the unwitting sender. This is, from example, an owner whose device has been taken over by a botnet[4], which is a type of malware that allows an attacker to take control over an affected computer. Bots are usually part of a network of infected machines, known as a "botnet", which is typically made up of victim computers that stretch across the globe or the owner of an account that has been hijacked or spoofed for the purposes of sending spam. These users and their computers may also suffer direct and indirect harm as a result. Intermediaries that are used to deliver and receive communications such as Internet Service Providers (ISPs) and communication platform service providers (e.g. social media, email providers, VOIP providers, etc.) are also impacted by spam traveling over their networks crowding out legitimate messages.

Spam affects the whole Internet ecosystem, as it wastes valuable network resources, often causes harmful use of a shared resource as well as inflecting reputational harm on message senders.
A suggestion was made to strike out or replace the term "regulation" as part of the Forum's title, as regulation and legislation are only two of many, possible tools that can be used to address the spam problem. On the other hand, other industry participants to the forum made a clear call for more regulation. This forum concludes that there is a strong reaction to the word "regulation" from the ISPs and other Internet related industry. At this point in time it is only possible to conclude that further debate is necessary around this topic.

b. Spam

The remainder of this document focuses on unsolicited electronic communications, often referred to as "spam", unless specified otherwise.

While there is no globally agreed definition of spam, most definitions tend to converge around "unsolicited bulk email[5]". The International Telecommunication Regulations (ITR) under the coordination of the International Telecommunication Union (ITU) calls upon member states to "endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services and to cooperate together in that sense"[6]. However, it is important to note that the term "unsolicited (bulk)

[3] http://issuu.com/ewipublications/docs/fighting-spam, K.F. Rauscher, Z. Yonglin (2011)

[4] 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.

[5] What is spam? http://www.internetsociety.org/doc/what-spam. In this report an overview of what spam is and the history of spam is presented in a concise way.

[6] Final Acts of the World Conference on International Telecommunications (Dubai, 2012) Article 7 - Unsolicited bulk electronic communications (http://www.itu.int/dms_pub/itu-s/oth/02/08/s02080000024502pdfe.pdf).

electronic communications” has a different meaning depending on the country and the approach it has taken to address the problem of spam. In other words, what spam is, is in the eye of the beholder.

One good example of why spam needs to be addressed can be found in the following remark:

> “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 want to receive”[7].

Spam is delivered to many different electronic communications platforms. For the mobile industry, this is done in the form of unsolicited text, i.e. SMS and MMS messages, which often contain fraudulent content, aimed at misleading users. Spam is also growing on social media (e.g. Facebook and Twitter). However ,social media spam and the issues that are caused by it have not been addressed to date in this Forum.

c. The cost of spam

The costs of mitigating spam are borne by consumers, the Internet industry and society at large. Spam also risks diminishing trust in doing business online, which has a direct effect on an economy. End users are directly affected because of the time spent on dealing with spam messages, the money spent on protective measures against e.g. spam and malware and the loss through fraudulent actions. Governments spend money on consumer awareness campaigns, legislative processes, regulatory and enforcement agenciesetc. Industry is affected in several ways. The cost impact of spam is significant for email service providers, which require increased storage capacity, faster processing capability, and access to higher levels of bandwidth to manage the ever-increasing volume of traffic. Internet Services, Hosting and Platform Providers invest in different protective measures, which are dealt with more extensively below. The whole industry works together to develop Internet standards, best practices and codes of conduct for their use. One example of a study that goes into detail on cost of spam is ‘The Economics of Spam’[8]. In the report it is estimated that American firms and consumers experience costs of almost $20 billion annually due to spam[9].

One of the comments made at the Best Practice session on unsolicited communications in Istanbul focused on the fact that all spam have one objective only: to make money for the spammer.

d. Background: the rise of “spam” and the rise of costs

The rise of spam follows the success of modern electronic communication (e.g. email). The speed with which, from circa 1995 onwards, email communication, soon followed by instant messenger services, fax to email 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

[7] What is spam? Internet Society

[8] ‘The economics of spam’, Rao, Justin M., and David H. Reiley. 2012.. Journal of Economic Perspectives, 26(3): 87-110 https://www.aeaweb.org/articles.php?doi=10.1257/jep.26.3.87

[9] Obviously this estimated figure is for the United States alone.

unprecedented. Spammers simply adapt to use the available technology to reap the potential illicit 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 delete the messages, the volume of messages crowded out legitimate email messages. Accordingly, the cost for ISPs and other intermediary companies grew through the rising number of complaints from customers and the demand for support centre capacity. Network operators faced the prospect of large volumes of traffic that "clogged up" network capacity caused by unsolicited Internet traffic, which needed to be addressed. As a result, a number of countries developed anti-spam laws. Industry developed technical traffic management measures to address spam such as filtering, blocking and operational best practices that address cooperative self-regulatory measures. The cost of spam rose accordingly, with costs for countermeasures largely being borne by ISPs, network operators and their customers.

With the success of email 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[10]", emails that suggest sending an amount of money with the promise of grand returns). With time, much worse emails were sent, such as phishing[11], 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 thus infect his device with malware. The already mentioned botnets made it easier to send spam in fast increasing volumes. Cost for spam mitigation rose accordingly.

e. Defining "spam"

In the paper 'Fighting spam to build trust'[12] it is noted that there are four attributes of spam that make for its potency. Spam is:

- Potentially viral, as there is little impedance to proliferation;
- Untraceable, as it is very difficult to identify the true originator;
- Automated, as computers can be controlled without their owners' authorization;
- Mutable, and preventative measures against spam are primarily reactive[13].

There are many different spam laws in the world, as it has already been shown. Harmonisation of these laws is highly unlikely due to differences in approaches and (a lack of) collaboration among all the players. However, there are some examples for countries that are contemplating drafting an anti-spam law to review as possible guides when developing their own approach. Currently, there is no comparative document that outlines the approaches taken to address spam by each country that has implemented a solution that could be used as a guide. This could be a topic for this forum to encourage in 2015.

[10] The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud.

[11] "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

[12] http://issuu.com/ewipublications/docs/fighting-spam, K.F. Rauscher, Z. Yonglin (2011)

[13] http://www.ewi.info/idea/fighting-spam-build-trust

The **European Union (EU)** Directive 2002/58[14], the so-called Directive on privacy and electronic communications, restricts spam to unsolicited commercial communications including email, automated calls, SMS text and fax messages. **The Netherlands** has broadened this to include ideological and charitable electronic communications[15]. In the EU, spam is approached from a privacy infringement point of view. The Directive only restricts the sending of spam. Legislation in **Australia, New Zealand and Canada** approximate the intentions behind the Directive and also focus on the consent of the sender: an opt-in regime.

The **Australian** anti-spam act[16] focuses on three main requirements. All messages must:

- be sent with consent (inferred or express);
- contain the name and contact details of the sender;
- contain a functional unsubscribe.

The **United States'** CAN/SPAM Act[17] does not address the sending of unsolicited electronic communications like the EU Directive and most other anti-spam acts do. It takes foremost measures against bad actors[18]. The Can/SPAM Act aims at protecting consumers and only forbids commercial email that is fraudulent, or was sent after the recipient requested the sender to stop. It includes rules prohibiting misleading headers and subject lines, requiring opt outs and appropriate labelling for adult content.

Industry, in stopping unwanted bulk emails from reaching its customers, arguably takes the broadest measures possible and filters out all unsolicited bulk sent emails as spam whether commercial or otherwise. As someone from the industry community posted to the BPF: "I rely on the definition of Spamhaus", which reads: "Spam is Unsolicited Bulk Email ("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"[19]. From comments in the group it can be determined that the Internet industry does more than the law requires, especially in the U.S., where it is allowed by law to send direct marketing communications until someone opts-out[20]. Responsible industry representatives presume that it is unwanted. Also it was pointed out that industry may not intercept spam in the same effective ways in all parts of the world. This is discussed further under "Regional differences" below.

Spam can also be defined by either regulatory or self-regulatory measures that a direct mailing company adheres to; e.g. the Australian Communications and Media Authority (ACMA) registered

[14] Directive 2002/58/EU of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[15] http://wetten.overheid.nl/BWBR0009950/Hoofdstuk11/111/Artikel117/geldigheidsdatum_15-08-2014

[16] http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366/

[17] http://www.legalarchiver.org/cs.htm

[18] See e.g. Sections 2.1.2 and 2.a.7.
http://www.gpo.gov/fdsys/pkg/PLAW-108publ187/pdf/PLAW-108publ187.pdf

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

[20] In the United States free, commercial, speech is recognised as having value, so cannot be restricted.

an industry code called the **'Spam Code'**[21] in 2006, which operationalizes how Internet and email service providers manage spam. ACMA enforces the self-regulatory rules. This is one example of many accepted practices and codes of conduct from around the world that can be examples for other countries to follow.

Several industry self-regulatory initiatives have been brought to attention. These initiatives all try to define a distinction between spam and legitimate bulk mail, so that it can be sent successfully and received by the intended recipients. The **Messaging Malware Mobile Anti Abuse Working Group** (M^{3}AAWG)[22] has developed an industry accepted code of conduct for bulk email distributors[23]. The **Groupe Speciale Mobile Association**[24] (GSMA) has developed a code of conduct for its members[25]. Both have been widely adopted by the respective industries. Several national Direct Marketing associations have developed national best practices that assist its members to adhere to the different regulations addressing the sending of direct mass mailings[26]. All come back extensively in section 3 of this report.

To conclude, three main conclusions can be drawn when defining spam that show main differences between different stakeholders.

1. In most countries that have passed anti-spam law, unsolicited commercial electronic communications is wider than just email and includes e.g. SMS, unsolicited automated calls, fax and social media messages.
2. The internet industry includes all other unsolicited bulk email, but non-email messages are mostly not covered.
3. Unsolicited bulk email can be other than commercial, which in most countries is not defined as unsolicited communications and may fall under other legislation or cooperative arrangements.

These conclusions led to comments from government agencies representatives that need further debate. Is the assumption correct that the Internet industry involved in anti-spam measures focuses on email only? Are we missing current anti-spam initiatives in the forum? If industry focuses on bulk messages, are they in any way involved in the fight against individual unsolicited messages?

It was noted in the comments that the term "commercial electronic message" is misleading. The term means different things in different countries. This leads to confusion. Also it is noted that commercial electronic email does not capture the discussion in this Forum. This has gone beyond spam, as seen from the traditional view on spam, as well as gone beyond spam as defined in anti-spam laws, but (ideally) captured in other laws. These topics all need further discussing.

f. Some metrics on spam to size the problem

[21] The code is successful. In fact the code may be deregistered soon because the market is sufficiently mature.
[22] In this document the current name of the organisation is used: M^{3}AAWG. It started as MAAWG in 2004.
[23] http://www.maawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2a-updated.pdf
[24] http://www.gsma.com/
[25] http://www.gsma.com/publicpolicy/mobile-spam-code-of-practice
[26] E.g. the U.K. Direct Marketing Association's code of conduct,

There is a multitude of reports available on the volume of spam, so called spam metrics. Reports originate from different sources[27]. However, there is divergence over the value of the reports in general, and disagreement among those who report on spam, about the scale of the problem as well as with regard to who the main perpetrators are or where they come from. It is unclear how such a discrepancy has arisen, however, suffice to say it would appear that inconsistent methodologies are applied[28].

Several participants in this Forum have stated that it is best to leave out the metrics topic altogether. It has been decided to keep the data, at least for this report, to capture the potential scope and size of the problem. Not so much as an undisputed truth, but for the fact that the presented facts and figures below are examples of what different actors see, record and publish on spam.

Having said this, recent reports and studies all indicate that the volume of spam messages 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. There is a rough consensus in this Forum that spam at this point in time constitutes circa 85% of all global email traffic.

In general, these reports 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. Another way of looking at these metrics could be the cost that companies and network providers spend on monitoring and trying to stop spam from reaching the end user. Beyond this general statement it is hard to quantify the true amount of spam generated or the actual financial impact.

Spam metrics often point to specific countries as being worse than others. 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 is just sent from there. The spammer and/or the one who ordered the spam to be sent is often in another country. We will return to examples of how countries have successfully taken specific measures against this abuse of resources within these countries.

What is of interest is that several statistics indicate that having spam legislation makes a difference. For example, the anti-virus vendor Trend Micro produces, on a daily basis, a world map with data that shows, per country, the percentage of spam set off against the total number of email messages[29]. 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 that have a law in place are (considerably) lower. Finland is on top, a country with a strict "spam", anti-botnet, disinfection legislation and a regulator, the Finnish Communications Regulatory Authority or FICORA[30], seeing to it that self-regulatory measures are undertaken by the ISPs[31]. This is relevant information. The shorter time a device is infected with malicious software or a botnet, the less spam

[27] Examples are threat reports by anti-virus vendors, e.g. Symantec, Sophos, Trend Micro, Kaspersky, etc. There are also statistics from M^{3}AAWG as seen by the largest ISPs (http://www.maawg.org/email_metrics_report). And statistics provided by Cisco, Spamhaus and reports from companies like Microsoft.

[28] 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.

[29] http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/index.html (Accessed 15 August 2014)

[30] The official Finnish name is Viestintävirasto.

[31] http://www.intgovforum.org/cms/component/content/article/116-workshop-proposals/1023-igf-2012-workshop-proposal--no-87-cross-border-cooperation-in-incidents-involving-internet-critical-infrastructure,

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 showed that, for 2013[32], on average 18% of spam messages advertised were on pharmaceuticals, 73% on adult content and dating. One in every 196 messages contained (a link to) unsolicited software ("malware") trying to infect the receiving device, while one in 392 spam emails contained a phishing message, aimed at obtaining personal (usually, but not necessarily, financial) data. The remaining percentages are e.g. commercial emails and stock (price manipulation) spam. However, Trend Micro sees a totally different division of spam emails in the first half of 2014. This is the top three: malware (20%), health (16%) and commercial emails (11%)[33].

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, e.g. consumers, (small and medium size) businesses, governments, Internet industry, financial institutions and others;
2. A spammer spams to make money or to obtain money that is not rightfully his;
3. The content and intent of spam in 2014 is more violent, intrusive and malicious than in 2000 when the first anti-spam laws were in the drafting process[34]. Spam is now used for all sorts of intrusions, the spreading of malware, fraudulent messages and phishing attacks to give a few examples.
4. A country ranking high in the spam lists often has a high number of Internet connections;
5. Often there is a (corresponding) high infection rate with malware for countries ranking high in spam lists;
6. There is a connection between lower scores and anti-spam legislation and;
7. An active regulator/anti-spam enforcement process.

g. 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**[35]. It identified several different stakeholders who each can take measures against spam. On both the individual and multistakeholder 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. M^{3}AAWG, Internet Engineering Task Force (IETF), London Action Plan (LAP) and the ITU. Without the involvement of all of these stakeholders, it is impossible to fight

[32] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[33] http://blog.trendmicro.com/trendlabs-security-intelligence/1h-2014-spam-attacks-and-trends/

[34] The ITU Discussion 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.

[35] http://www.oecd.org/internet/consumer/36494147.pdf

spam successfully[36]. Below, under Section 3, the main recommendations of the OECD Toolkit are presented.

Most stakeholders in this Forum stressed the need for cooperation and several have already found ways to cooperate. There is general consensus on the need to cooperate, it is the form(s) this can or should take which is not always clear. This is a topic that can be singled out for further debate.

h. 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. Multistakeholder dialogue, cooperation and partnerships could be improved or invited to start so that use of these tools and best practices can be shared.

2. Regional specificities observed (e.g. Internet industry development)

This section of the report is as diversified as there are regions around the globe. Topics brought forward by the Forum's members focus on diversity in Internet access, (the absence of) spam laws, (self-) regulatory measures, costs and effects of spam. Most likely this part of the report is not complete, just as the Forum in this short time span was not able to find all necessary data to support its findings in a more comprehensive way. The Forum is able to present first findings of regional specificities and present some results that suggest a way forward in different regions as there are still regions with limited access and exposure to the Internet.

a. 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 their Internet connectivity. Regions with previously limited connectivity might become a new source for spam and/or a new target for spammers as they progress their infrastructure deployment and access to the Internet. This came into the public's eye most significantly at the World Conference on International Telecommunications (WCIT) in 2012 in Dubai, when developing nations called for active measures against spam[37].

Most developing economies are in the process of expanding their ICT infrastructure. This results in growing numbers of people and organizations with access to those infrastructures, including all chances and opportunities access offers. The downside is that the number of risks also grow; including the possibility that the infrastructure will invite attention from undesirables, both with an intention to target citizens in fraudulent activities and to harness the infrastructure for their own operations. Often this occurs before any sort of (self-)regulation is debated let alone implemented,

[36] 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.

[37] http://www.itu.int/pub/S-CONF-WCIT-2012/en

while security products may be harder to get by due to cost. However, it should be noted that enhanced ICT infrastructure allows those in isolated economies to participate more easily in the digital economy offering and/or exporting services in a low cost and efficient fashion.
Countries with less bandwidth availability may suffer from congestion and significantly higher costs where there is major incoming and outgoing spam traffic that crowds out legitimate traffic.

b. Differences in anti-spam laws

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, Lithuania, Estonia, a few other EU countries and Chinese Taipei are also known to have implemented anti-spam legislation. The list may therefore not be complete[38]. Nevertheless, there are still many jurisdictions that do not make spam illegal, which is the main difference between countries.

The differences in anti-spam laws between countries have been dealt with extensively above and do not need repeating under this section. However, it was noted that there are (many) other laws dealing with fraud and criminality in the offline world. These apply or should apply to online world behaviour also.

c. Regional differences in effectively combatting spam

Spam hardly reaches the inboxes of users in developed countries anymore because of successful counter measures. 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[39];
- 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 users a feedback process to report unsolicited spam.

Unfortunately, none of these measures have the desired effect of stopping the most brazen of spammers[40]. They did cause several relevant partners in many developed countries to no longer see spam as a major problem because measures had been developed to manage the impact. According to comments from several Forum participants, it has led to governments losing interest and being absent from the present debate. The call for them to enter this Forum was convincing enough to

[38] 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. 'Countering spam: 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.

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

[40] 'A Two-Tiered Registry System to Regulate Spam', Shelley Cobos (UCLA, 2003)

conclude that there is a rough consensus on the different roles governments have to play in fighting spam, from awareness raising of end users to effective spam legislation, including an enforcement agency with effective sanctioning powers, and a consumer protection process for awareness and education. How much regulation really is in place?, was a question asked in different ways by participants.

This Forum has concluded also that legislative 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. education, 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. It was concluded that there are considerable differences between regions and that these differences can also have a negative effect on cross border cases and cooperation among existing enforcement agencies.

There are differences between countries in the way a government agency can cooperate with colleague agencies at the national, regional and international levels[41]. Nonetheless, the London Action Plan[42] has facilitated cooperation and a cross border dialogue among government agencies involved in end user protection and enforcement within the international anti-spam community[43].

d. 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[44]. The ISP and telecommunication industries started to organise themselves around the topic[45] and discussed, developed and implemented technical and operational best practices to address the problems of spam.

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 used approaches used by many network operators in fighting spam[46].

Several countries have taken different measures that drove spam volumes down considerably. Japan in 2005 blocked access to Port 25 from dynamic IP addresses[47]. Brazil's CERT and industry have taken measures along the same lines[48]. The Netherlands, from May 2004, had an enforcement agency with investigative powers tool and budget. This led to a drop of identifiable Dutch language spam of 85% in the first six months of the inception of the anti-spam law[49]. In December 2009, China obliged anyone who registered for a .cn country code domain name to hand over personal data

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

[42] Londonactionplan.org

[43] Also look at ITU Discussion Paper. 'Countering spam: How to craft an effective anti-spam law'

[44] As shown by (self-)regulatory, technical, security and legislative measures undertaken by different stakeholders.

[45] E.g. M^{3}AAWG and Direct Marketing Associations in different countries

[46] http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf

[47]Present Situation and Problems concerning the Consumer Policies for Telecommunications Services, Ministry of Information and Communication June 2009, http://www.soumu.go.jp/main_sosiki/.../090618_1.pdf

[48] See e.g. 'Port 25 Management in Brazil: Overview and results', of 7 May 2013, a presentation by Cristine Hoepers and Klaus Steding-Jessen of CERT-Br

[49] http://www.spamvrij.nl/nieuws/persbericht.20041228-nl.php

proving identity[50]. China disappeared immediately out of spam metrics of the time, causing Russia (.ru) to rise sharply[51]. Spammers en masse left China because of the measure. We have seen Finland's anti-bot measures above.

This Forum acknowledges that not all examples mentioned here are uncontested, but chose to present all examples that have been provided by participants so that the regional diversity of the measures can be noted. Each country mentioned used its own approach; the result shows that different measures can have effects. The common denominator is that in all mentioned approaches more than one stakeholder is involved.

The technical Internet community has also drafted proposals for techniques to address the problems of spam. Over the past decade and a half several solutions have been presented in the form of Requests for Comments (RFC) within the IETF[52], e.g. an anti-spam protocol was set up. Below, in section 3, an extensive overview is presented of some of the anti-spam solutions.

There are signs that collaboration, technical standards and best practices that Internet communities have implemented in the developed world may not have been adopted in the developing world causing a disparity in the tools used to combat the problem of spam. Data supporting this assumption is largely missing at present. This is a topic that deserves more attention.

e. 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, abuse and help desks and investments in protection and recovery. The way organisations and people are able to respond to the challenges spam poses is not the same around the globe.

A study on cost [53] published in 2008 could still be relevant for developing nations. 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 employee per year were lost due to spam. With successful spam management and filtering techniques this study 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 or already has relevance there. This is underscored by the presentation Animesh Bansriyar, an architect at Cloudmark, gave at the India Anti-Abuse Working Group[54].

f. 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

[50] http://garwarner.blogspot.nl/2009/12/china-changes-registration-rules-will.html or in the Shanghai Daily: http://en.ec.com.cn/article/newsroom/newsroomindustry/200912/947426_1.html?COLLCC=1639998043&

[51] http://www.eweek.com/c/a/Security/Russian-Spam-Domains-Increase-After-China-Tightens-Domain-Registration-Rules-372038/

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

[53] 'Measuring the Effect of Information System Technologies in Organizations' (Bonn, 2008) http://ftp.iza.org/dp3755.pdf

[54] http://www.m3aawg.org/system/files/M3AAWG%20Animesh%20bansriyar_0.pdf

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 mass use, 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.

A topic for further debate could be how economies, who are mature in terms of dealing with the spam problem, could be used as models to forecast the situation in developing economies. Further it might be useful to indicate what could/would be done if finances were available in those economies who lack the ability to effectively address the spam problem.

3. Existing policy measures and private sector initiatives

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, to mitigating spam. This section needs a subdivision as one part looks at legislative initiatives, while others are aimed at self-regulation from an industry perspective.

a. Regulation

i. Intergovernmental actions

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**[55] as a framework of recommended policies and measures addressing regulatory approaches, enforcement cooperation, industry driven activities, technical solutions, education and awareness initiatives, spam measures, and international cooperation and exchange[56].

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 included 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.

[55] http://www.oecd.org/internet/consumer/36494147.pdf

[56] The OECD published a review on 2012: http://www.oecd-ilibrary.org/science-and-technology/review-of-the-2006-oecd-recommendation-on-cross-border-co-operation-in-the-enforcement-of-laws-against-spam_5k95tn9rmhq6-en

The **London Action Plan**[57] 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 Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Ministerial Meeting issued **"APEC Principles for Action against Spam"[58].**

The report 'Fighting spam to Build Trust provides two consensus recommendations and 46 voluntary best practices for international spam fighting[59].

The issue of spam was thoroughly discussed among participants at the WCIT held in December 2012 in Dubai. This conference updated the **International Telecommunication Regulations** (ITRs) – an international treaty setting out general principles which relate to the provision and operation of international telecommunication services offered to the public as well as to the underlying international telecommunication transport means used to provide such services. Article 7 of the amended ITRs, which will come into force among the 89 signatories on 1 January 2015, reads:

> "Member States should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services. Member States are encouraged to cooperate in that sense"[60].

The ITU Discussion Paper '**Countering spam: How to craft an effective anti-spam law'** 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. The ITU gives a clear advice on how to draft a new generation of spam laws that go "beyond mere sentiment to real action"[61].

The **ITU Development Sector Study Group 2 on "ICT applications, cybersecurity, emergency telecommunications, and climate-change adaptation"**[62] focuses, among other areas, on building confidence and security in the use of ICTs, including combatting spam. More specifically, within the framework of **Study group 2 Question 3/2 (former Q22-1/1) "Securing Information and Communication Networks. Best practices for Developing a Culture of Cybersecurity"**, 24 best practices were identified to address the protection of end-users as well as the network against spam malware and other cyber threats[63]. These best practices are primarily for use by Internet Service Providers that provide service to consumer end-users on residential

[57] http://londonactionplan.org

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

[59] http://issuu.com/ewipublications/docs/fighting-spam, K.F. Rauscher, Z. Yonglin (2011)

[60] http://www.itu.int/pub/S-CONF-WCIT-2012/en

[61] ITU Discussion Paper. 'Countering spam: How to craft an effective anti-spam law'

[62] http://www.itu.int/net4/ITU-D/CDS/sg/index.asp?lg=1&sp=2014&stg=2

[63] See Annex D of the 2010-2014 Study Period Report: http://www.itu.int/pub/D-STG-SG01.22.1-2014

broadband networks, but may apply to other end-users and networks as well. For the study period 2014-2018, approaches and best practices for evaluating the impact of spam within a network, and the necessary measures, including mitigation techniques, that developing countries can use, will be under study.

Furthermore, the **ITU Standardization Sector (ITU-T) Study Group 17 "Security",** in collaboration with the relevant organizations, develops technical recommendations, with a view to exchanging best practices and disseminating information through joint workshops, training sessions, etc. **Study Group 17 Question 5/17 "Countering spam by technical means"** studies the range of potential technical measures to counter spam as it relates to the stability and robustness of the telecommunication network. So far, 11 spam-related Recommendations and Supplements have been developed under this Question[64].

In 2014, the 23rd Ordinary Session of the Summit of the African Union[65] 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)[66].

ii. Governmental action at the national level

Several countries, as shown above, have implemented an anti-spam law, one of the available tools to combat spam successfully. 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.

Governments also assist in setting up public-private partnerships whose goal is to drive down spam volumes (e.g. via national support centres[67] 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[68].

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.

[64] http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/q5.aspx

[65] This BPF strives to present more regional initiatives in the near future.

[66]http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf

[67] See e.g. https://www.botfrei.de/ , https://www.abuseinformationexchange.nl/ , http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative

[68] www.signal-spam.fr

iii. Spam enforcement

There is considerable variation in the organizations and government agencies 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 etc.[69].

There appear to be a number of impediments to successful cooperation across the mentioned organisations. Some examples:

- Enforcement tools may be stronger or weaker depending on how the responsibility has been stated in the spam legislation. 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.
- There is a lack of technical expertise and/or resources.
- 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.

Another important challenge is the attribution of spam, e.g. a clear difference between the sender of spam and a 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.

Also, 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. For example, the case of the Dutch Independent Post and Telecommunication Authority[70] (OPTA) against "Dollarrevenue", although a malware spreading case, has implications for spam enforcement. The fine was annulled in court because of territorial issues (and attribution)[71]. Not having a level playing field between agencies is a major impediment to fighting spam with a chance at success[72].

On top of this, several agencies found that with the initial success of fighting "the low hanging fruit" of spammers, now that cases involving more serious or harmful spam have to be dealt with, there is no one at policy level to address this. 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 seem to stand up to the current challenges at hand.

[69] 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 e.g. http://londonactionplan.org/members/

[70] 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.

[71] http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:CBB:2013:CA3716

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

Perhaps the hardest challenge is to make a long-lasting impact on the well-resourced criminally motivated spam, particularly where the conduct is undertaken across multiple borders. The LAP/ M^3AAWG 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[73].

Enforcing spam is only one of the possible approaches to fight spam in a successful way. More precisely, most participants involved in this Forum see it as the last resort for when all other counter measures fail.

A consenting position was identified by a participant in that "there needs to be a discussion around existing laws that could be used to combat spam in the online world. Without a clearer definition and a recognition of both the costs and the benefits of that choice, (*the participant*) cannot agree to the implied conclusion that making spam illegal is a preferred policy outcome. In particular when spam can be defined in ways that unduly restrict lawful speech".

iv. End users

Over the past years, most stakeholders have realised that the use of the Internet comes with risks, along with the benefits. Together with this realisation comes the call for a greater focus on ensuring digital literacy. End users would benefit from a better understanding of the value to themselves and other Internet users concerning e.g. spam, privacy, security tools and regularly patching software updates etc. From this grows a better understanding of the impact that (in)action has on their own and others' online security.

Debates on Internet safety sometimes focus on the need for educating end users. The fact that there are no rules for Internet users is seen as one of the impediments to addressing spam successfully[74]. 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 forbidding spam.

It was identified that the Internet's system of permissionless innovation is what has enabled the Internet's growth and success to date.

There is a need for further debate on if, and if so, on how, user education and/or rules for users could prevent or render more harmless, spam and other malicious online conduct.

[73] http://londonactionplan.org/wp-content/uploads/2012/12/Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf, page 44. The document is actually under review and expected to be updates in late spring 2015

[74] 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 email: http://www.geek.com/news/charging-for-email-will-stop-spam-551697/

b. Self-regulation

i. 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 level, 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 email filters include organizing incoming email and removal of spam and computer viruses[75]. The higher up in the network the traffic is filtered for spam, the less the end user notices it and the lower the cost for the end user is.

Constant refinement of these techniques is needed to endeavour to make sure that the number of unsolicited 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. There is an inherent market incentive for industry across the entire sector to stay one step ahead of spammers, both to provide a better user experience for their users as well as to lower their own costs associated with spam.

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[76]. Discussions within this 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"[77]. 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 organizations on the Internet will block or filter out all traffic coming from that address. Blocklists from organizations 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.

M^{3}AAWG is comprised of members from ISPs, network operators and the direct marketing industry. It 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". The results are freely available on M^{3}AAWG's website[78]. From being an American centric organisation at the start in 2004, M^{3}AAWG branched out to Europe first and recently has set up an Indian chapter[79].

[75] http://en.wikipedia.org/wiki/Email_filtering

[76] Source: http://en.wikipedia.org/wiki/Anti-spam_techniques

[77] The term "blacklisting" is used also. The terms are synonymous.

[78] www.m3aawg.org

[79] Presently, at M^{3}AAWG meetings, U.S. representation is below 50%.

In 2006 **GSMA** adopted a **code of conduct** for the mobile industry on how to handle spam[80]. This code dealt with:

- Anti-spam provisions in contracts with third parties;
- Commitment to cooperate between operators national and international level;
- Commitment to educate consumers;
- Commitments to filter out spam and;
- To shut down SIM cards once they are identified as spam sources.

These measures led to a second step, the **GSMA Spam Reporting Service** for mobile operators. This tool has three main functions:

- It captures reports from subscribers;
- It analyses the reports and matches them against known attacks
- It includes a dashboard, which displays in real time statistics showing the various spam attacks, the level of threats where the spam attack has originated and destinations.

In general, among industry there is a large level of trust that has been established, 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.

The U.S. Can Spam act allows civil right of action against spam[81]. Several companies have used this clause to successfully fight spam through a court and take down botnets, often in cooperation with (inter)national law enforcement and other involved companies, e.g. hosters. The most eye-catching ones are by Microsoft[82], although there is no consensus that this approach is a best practice, due to negative effects to many legitimate users.

ii. Technical Internet community

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

1. **Internet Engineering Task Force[83].** The IETF 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)[84], RFC 6561 (Recommendations for the Remediation of Bots in ISP

[80] http://www.gsma.com/publicpolicy/mobile-spam-code-of-practice
[81] Can/Spam act (2003), Section 7, g.1
[82] See e.g. http://www.microsoft.com/en-us/news/press/2013/jun13/06-05dcupr.aspx
[83] http://www.ietf.org/
[84] http://tools.ietf.org/pdf/rfc2508.pdf

Networks)[85] and to provide information on methods being used by particular service providers, such as RFC 6108 (Comcast's Web Notification System Design)[86]. The IETF has also developed several technical approaches to help combating spam. One of them, DomainKeys Identified Mail (DKIM)[87], 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[88]), 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 maintained, the group ceased activity in 2013, an Anti-Spam Research Group (ASRG)[89] that investigates tools and techniques to mitigate the sending and effects of spam. Its focus was 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[90] 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[91]. Another project worth mentioning is DMARC. This is an approach leveraging the IETF SPF and DKIM work on email authentication to allow ISPs and other receivers and senders of email[92].

2. **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[93].

3. **CERT-BR.** CERT-BR, the Brazilian Computer Emergency Response Team, reported on different self-regulatory measures implemented by the Brazilian Internet industry, which drove spam coming out of Brazil down considerably.

[85] http://tools.ietf.org/html/rfc6561

[86] http://tools.ietf.org/pdf/rfc6108.pdf

[87] DomainKeys Identified Mailtext 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

[88] 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

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

[90] "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

[91] http://tools.ietf.org/html/bcp38

[92] http://dmarc.org

[93] http://www.internetsociety.org/doc/combating-spam-policy-technical-and-industry-approaches

iii. Direct marketing community

Direct marketing associations took it upon themselves to draft self-regulatory binding rules. For example, the U.K. code of conduct 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"[94]. These codes of conduct can e.g. aim at more transparency and identify steps against offending members.

Brazil provides the example of a code of conduct without legislation in place[95]. A question that can be asked is whether there are other examples in place like Brazil's and to compare the effects with countries with an underlying legislation.

These examples of best practices are freely available from the (websites of respective) direct marketing associations and can be adopted by any organization that wishes to do so.

As mentioned before, the direct marketing community has worked together with ISPs to develop best practices, operational tools and agreements that allow direct marketers to send legitimate bulk email, which will arrive at the intended destination[96]. **M^{3}AAWG created a Senders' Best Practice** document as well as being instrumental in the cessation by many legitimate senders of commercial email of the practice of e-pending.

Governments at national or regional levels could stimulate self-regulatory processes like the examples provided above as a part of their anti-spam strategy, like the GSMA actively stated concerning the further adoption of its own self-regulatory measures. The previously provided examples of Finland and Australia can be other examples of a way forward.

It was noted that bad actors are not stopped solely by self-regulation alone. Several participants advocated an anti-spam law including an enforcement agency with adequate powers to enforce in those cases where self-regulation is not adhered to or has no effect. This tiered approach is another topic worth discussing further.

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 taken action upon, no company wants to be associated with spam"[97].

[94] http://www.dma.org.uk/the-dma-code

[95] http://www.capem.org.br. More general information can be found here http://www.antispam.br/en.

[96] http://www.m3aawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2a-updated.pdf

[97] 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".

iv. Financial institutions

In some countries, financial institutions also play an active role in addressing spam, such as with anti-phishing campaigns: the focus there is on helping customers recognise a misleading or fraudulent email and/or message. This form of customer education could be an example of a best practice for other countries.

v. Spam Delivery Mechanisms - Anti-botnet initiatives

In previous sections, the link between botnets and their underlying system of infected devices and the sending of spam has been pointed out. The discussion on the Forum brought forward that the topic of spam mitigation needs to include the content of spam messages and botnets as part of this report.

Several countries have opened botnet mitigation centres or have started initiatives to do so at national level. At present e.g. **Australia, Germany, Switzerland, South Korea and The Netherlands** have active centres that gather information on infected IP addresses and assist end users in cleaning up their devices. Countries like **Belgium, France, Spain, Italy, Luxemburg** and Croatia have recently announced national initiatives. At the EU level **ACDC, Advanced Cyber Defence Centre**, co-financed by the European Commission, is establishing public-private participation and cooperation at the EU level[98]. In **the U.S.** there is a code of conduct between ISPs on how to handle bots[99].

This topic may become even more pressing now that more and more devices come online: the coming of "the Internet of Things". However, there are many issues around national and international cooperation concerning the sharing of personal data and specifically IP-addresses. In order to alert an ISP that it has an infected device on its network in an effective way, an IP address, usually including a time stamp, needs to be provided. This way the ISP can alert his customer of the infection and pass advice how to clean the device up. If this is not allowed due to restraints in the privacy law[100], the user cannot be alerted nor assisted and hence remains vulnerable to threats and his device abused to harm or threaten others.

A representative from the hosting industry stated that there is a need for active abuse desks. Some ISPs or hosting companies do not have a point of contact where complaints on (violent) behaviour from their network can be reported to or they may have them but do not respond to calls. This is a topic that is discussed for years within the RIR communities but to unsatisfactory effect[101].

Also there are no (adopted) best practices on security by design for chips, hardware and software that allow for more secure connection of all devices coming online.

This Forum notices that the discussion to look at spam as the delivery mechanism for bots is not finalised and marks it for further debate.

[98] http://www.botfree.eu/

[99] https://www.maawg.org/abcs-for-ISP-code

[100] This topic also came forward in the BPF on CSIRT.

[101] See e.g. http://www.ripe.net/ripe/groups/wg/anti-abuse

vi. Spam activists

In several countries there are individuals and private organizations who collect data on spam or phishing and publish the results on websites. Some have become sources of influence, like the Spamhaus Project[102], the Coalition Against Unsolicited Commercial Email (CAUCE)[103] and the Anti-Phishing Working Group (APWG)[104], 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 organizations like these in their respective countries, as they are most likely to be a good source on spam activities.

Where local experts are not identified, consideration should be given to creating training and support to stimulate the emergence of such expertise on a local basis.

c. Summary of possible solutions

In this section a wide range of (proposed) solutions is to be presented. The Best Practice Forum on spam is collecting information on solutions and tools that can be used to address the problem of spam, however this list is a work in progress and does not endorse any particular tool or approach as well as it needs to be noted that this is not an all inclusive list of options and possibilities for combating spam. The list of tools and solutions will be provided in the next report of this forum.

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.

a. Government leadership

Governments, by taking the lead in facilitating anti-spam discussions, assist industry in determining what is legitimate messaging as well as in facilitating the discussion on solutions and self-regulatory measures. An anti-spam law that defines spam provides clear direction of what is legitimate messaging to direct marketers and users. Additional items are also beneficial to consider, such as the fact that any approach with a minimal hint at enforcement drives away most in-country spammers. Combined, the definition and enforcement capabilities provide the tools for a government to address cross border spam with other governments.

b. Industry leadership

The technical measures that the Internet industry have taken upon themselves to use, to manage their network such as filters for email traffic, have proven to be successful.

[102]http://www.spamhaus.org/
[103] http://www.cauce.org/
[104] http://www.antiphishing.org

The process that the IETF, M^{3}AAWG and GSMA have in place leads to development of internet standards, best practices, codes of conduct and identifies tools and operational processes that work well. These materials are openly available for use by all interested parties.

c. Spam activists

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

5. Unintended consequences of policy interventions, good and bad

a. 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, right after CyberBunker was added to a Spamhaus blocklist[105], which resulted in CyberBunker's email messages being blocked on most ISP networks. Network operators who implement anti-spam measures could also be subject to threats and attacks from spammers who do not like to have their traffic restricted or blocked.

b. 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) email may still get through. Also, there may be a temptation to use such technology for censorship purposes.

c. 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. Spam filtering can also limit the delivery of legitimate messages causing harm to both the sender and the intended receiver of the message. In considering this issue, it is also important to understand that any solution to address spam mitigation must also be aware of the need to allow for the flow of all legitimate messages without restriction or adverse effects to an individual's privacy.

d. 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").

[105] https://en.wikipedia.org/wiki/The_Spamhaus_Project#CyberBunker_dispute_and_DDoS_attack

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[106].

e. 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 free speech and privacy;
- the impact on innovation and cross-border trade;
- the ability to access information, etc.

They should be evidence-based and draw upon the interests and expertise of all relevant stakeholders.

6. Unresolved issues where further multistakeholder 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 multistakeholder 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 perpetuate their malicious and fraudulent activities.

Below are some specific areas that may merit from further collaborative multistakeholder discussion:

- How to assist application and service providers to effectively implement technical anti-spam measures;
- How to fairly and equitably share the costs and benefits from mitigating against unsolicited communications, particularly where such activities are transnational;
- How to defend against and recover from retaliation by malicious actors;
- How to empower users to help contribute to specific and overall mitigation of unsolicited communications;
- How and where to discuss development and ensure 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;

[106] "An economic problem in which every individual tries to reap the greatest benefit from a given resource. As the demand for the resource overwhelms the supply, every individual who consumes an additional unit directly harms others who can no longer enjoy the benefits". www.investopedia.com

- There is a need for a further inventory of the ways botnets are fought, as well as ways for different stakeholders to cooperate on this topic and under which circumstances they are allowed to exchange (privacy sensitive) data[107].
- Creating a competitive environment and level playing field for application and service providers;
- How to ensure respect of individuals' rights of freedom of expression and expectations of privacy while mitigating against unsolicited communications;
- Improving cross-jurisdictional technical and legal mitigation against unsolicited communications (including law enforcement);
- How to ensure effective and trusted cooperation between different stakeholder (communities) that strengthen each other's resolve in fighting spam.
- Impediments to effective development and implementation of anti-spam policy;
- There is strong disagreement between the need for regulation or not. There is a need to clarify the need for as well as the resentment against regulation. For example, is it necessary to make a clear distinction between regulation of the Internet and regulation and/or the enforcement of unsolicited communications?
- 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[108].
- Trust is one of the most elementary prerequisites for organizations 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;
- There is a whole underground, digital economy. More knowledge on this economy could be shared among stakeholders, in order to identify weaknesses in these "commercial" offerings.

These items in short sum up all the challenges mentioned above. Once distilled into the most elementary wording, the following sentence provides 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 unsolicited 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"[109].

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

[107] This outcome is not unlike the outcome in the CSIRT BPF. It makes sense to combine this specific topic in the future.

[108] 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.

[109] ISOC Paper: *Understanding Security and Resilience of the Internet* - http://www.internetsociety.org/doc/understanding-security-and-resilience-internet

There is no "silver bullet" and there will always be some level of unsolicited electronic communications. In fact, striving for 100% may have negative consequences for the end user. 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 text 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 person's or company's on- and offline security. Different stakeholders address the effects in different ways. Sometimes through regulation, often through successful industry developed self-regulatory processes. It is also possible to identify areas where all 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 collection of good practices across communities, regions or globally. A comparison between anti-spam laws, including effectiveness of measures and tools, is to be recommended. Challenges around international cooperation, data sharing, territoriality and jurisdiction need to be reviewed and addressed (again). Such reviews need active involvement of governments, privacy bodies and others who are invited to join this Forum.

This Forum made clear that anti-spam agencies and industry face new and big challenges concerning spam. At the same time, there are indications that governments in developed countries are not focusing on the topic of spam, while austerity in public finances brought budgets to fight spam down. However, government expertise in addressing the problem of spam is an important part of the solution from several angles, as shown in this report. Finally, expertise needs to be shared with broader communities who are just starting the journey of what needs to be done to address their problems with spam, for which expert resources and capacity building will need to be made available. 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 are not equipped to deal with them, other laws are involved, but these forms of fraud and other economic crimes do not always get priority from police. Nor is cooperation between agencies established easily.

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 multistakeholder dialogue

Further multistakeholder dialogue in this Best Practice Forum could focus on:

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

b. **Common understanding of solutions**. The challenge here is that there is a whole array of possible solutions (technical, policy, economic, financial, 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.

c. **Understanding of the differences between common and individual costs versus common and individual benefits when taking appropriate measures**. The technology, policy, economic and social building blocks vary in the costs and the benefits they bring individually, for example to a company, institution, user etc., and to the common good of the global Internet and users in general. There are signs these are misbalanced. Understanding these factors and how they are (not) aligned with the needs of governments, Internet users, the business objectives of network operators and other stakeholders and how to share the costs and benefits between them fairly and equitably is crucial for sustained improvements in addressing unsolicited communications.

d. **Ability to assess risks**. The ability to properly assess risks, including risks to the whole Internet ecosystem, can assist in determining the tools and approaches needed. 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.

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

f. **The difference between the developing and developed world**. It is important to understand that there is a difference in the challenges 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. How can existing, successful anti-spam measures be used as models to follow or implement?

g. **Clarification on consumer education, regulation, enforcement and rules.** There is a need to define and make an inventory of resentment against governmental involvement concerning the fight against spam, as well as the reasons behind the call for more regulation and the effect of both stances.

h. **Understanding of new spamming techniques**. New techniques could be presented and explained to governments and agencies on a regular basis, so that they can focus on solutions and educational processes.

i. **Understanding of the business case of spammers**. Most measures discussed here focus on reactive prevention in one way or another. Could a better understanding of the business case lead to forms of offensive actions against (the tools and finances of) spammers and make a difference? If so, which stakeholders need to be(come) involved in this sort of actions?

j. There is a need for a better understanding of data protection and privacy regulation in the face of fighting spam and botnets. A major challenge is the exchange of privacy sensitive data in general and especially between public and private entities, in the fight against (one of the main causes of) spam. It is of utmost importance to be able to share relevant privacy sensitive data, like IP addresses, between involved actors. However, there are still important questions and safeguards that need answering, respectively solving, before involved parties on the public and private side can cooperate in the fight against spam and botnets.

k. The balance between fighting spam, freedom of speech, privacy, innovation and doing business. There are thin lines between these elements. Can the different stakeholders find ways in which all can act according to their respective roles, while at the same time strengthen each other's resolve?

List of contributors

Lead Experts:

1. Christine Hoepers
2. Karen Mulberry

Contributors[110]:

1. Betsy Broder
2. Julia Cornwell McKean
3. Richard D.G. Cox
4. Sarah Falvey
6. Cristine Hoepers
7. Kolubahzizi T. Howard
8. Karen Johnson
9. Simon Kaheru
10. Tobias Knecht
11. Eliot Lear
13. Michele Neylon
14. Michael O'Reirdan
15. Ernesto Perez
16. Myla V. Pilao
17. Alejandro Pisanty
18. Suresh Ramasubramanian
19. Karl Frederick Rauscher
20. Shreedeep Rayamajhi
21. Neil Schwartzman
22. Aparna Sridhar
23. Yiannis Theodorou
24. Maarten Van Horenbeeck

Editor:

Wout de Natris

[110] This list includes:
- the participants in the online discussions held via the dedicated mailing list;
- the contributors who commented on the online review platform (those who have not indicated their full names when making comments were not included in this list).
- panellists in the Best Practice Forums session held during the IGF 2014 meeting.