

COMBATTING SPAM: INTERNATIONAL BODIES RECOMMENDATIONS

Introduction

SPAM represents a major annoyance and threat to ICT applications users and is spreading into all means of communications like mobile phones, facsimile transmissions, and SPAMmers are always on high-alert to exploit any new technology in order for them to achieve their goals.

Many countries, regional and international organizations, bodies, and working groups have taken steps to deal with the issue of SPAM. Anti-SPAM policy frameworks have been used in a number of countries to combat SPAM and many other countries are considering developing such frameworks.

When developing the Anti-SPAM Policy Framework for Saudi Arabia, a list of international bodies were identified and studied. Examples of those international bodies are: the Organization for Economic Co-operation and Development (OECD), the International Telecommunication Union (ITU), the Anti-Phishing Working Group (APWG), the Messaging Anti-Abuse Working Group (MAAWG) and others.

Thus, this article reviews, examines and extracts the best practices developed by the various international bodies in the following areas:

- Regulatory approach;
- Enforcement cooperation;
- Industry driven initiatives;
- Technical solutions;
- Education and awareness initiatives;
- SPAM measurement; and
- International Cooperation and Exchange.

Regulatory

The development of anti-SPAM legislation that tackles SPAM is fundamental. Legislation sets clear directions on what is allowed and what is not allowed. Since SPAM horizontally spans multiple areas, it touches upon telecommunication services, consumer protection, security, and privacy, at national and cross-border levels.

The anti-SPAM regulatory framework has multiple sub-components and according to OECD, it is recommended that the anti-SPAM regulatory framework is broken down into elements which should be considered as far as possible, taking into account each country's institutional and legal framework. These elements are: Technical elements, consent, privacy, commercial elements, bulk, content (fair trade, criminal or pornographic content), damage, requirements for legitimate messaging, exemptions or restrictions, and address harvesting and dictionary attacks. Even with these almost agreed-on elements in place, typically we find zones of divergence in legal approaches to spam. These differences often derive from diverging views on what constitutes permissible communication or the most efficient way to achieve enforcement. Examples of points of divergence are: the consent requirements: shall the consent be obtained prior to sending a message? Is one message considered as SPAM? Or only if sent in bulk? Enforcement, that is, who is permitted to recover for or prosecute violations of the law and, in particular, whether private entities such as ISPs and SPAM recipients, may recover damages?

Unfortunately, there is no common definition for SPAM and according to ITU and OECD, there are widespread typical features distinguishing a SPAM message, namely: an electronic message, with false or hidden origins, having non valid unsubscribe option, carrying illegal or offensive content, utilising of addresses without the owner's consent, and sent in bulk or repetitively.

What outcomes should be achieved by the anti-SPAM legislation? And what are the characteristics of a successful anti-SPAM legislation?

According to OECD, an anti-SPAM legislation should preserve the benefits of electronic communication, prohibit and take action against SPAMmers, and reduce the amount of SPAM. Moreover, it should conform to four general principles: Simplicity, effective enforcement, having appropriate international linkages, and providing a clear policy direction where the main objectives of the national and international anti-SPAM policy are outlined at an earlier stage and need to underline the entire governmental strategy.

In conjunction with OECD recommendations, ITU advises that anti-SPAM law should:

- Focus on content with commercial nature;
- Ban fraudulent or misleading messages;
- Prohibit concealing or falsifying a message's sender, advertiser, or routing information;
- Draft regulations covering Internet communication generally rather than specifying applications such as email;
- Require senders to provide recipients with unsubscribe facility, respect the recipient's requests, and prevent senders from exchanging or selling addresses or recipients who unsubscribe;
- Prohibit address harvesting and dictionary attacks, along with software tools specifically tailored to these purposes; and
- Seek to standardise labelling requirements.

Enforcement

According to OECD, enforcement is a fundamental issue, which, if not dealt with appropriately, can make a good piece of legislation useless. For this reason, it is recommended by OECD to put in place an effective sanction regime and appropriate standards of proof. In addition, appropriate powers and resources need to be allocated for enforcement authorities.

ITU and OECD recommend that countries should establish SPAM enforcement authorities. Mainly, one agency should be assigned as the nodal enforcement agency and serves as a coordinator at the national level among other national enforcement agencies (if existing) and as a contact point for foreign authorities to facilitate cross border co-operation. SPAM enforcement authorities should have the necessary authority and investigative power to obtain evidence sufficient to investigate and take action in a timely manner against violations of laws targeting the senders of SPAM and the individuals or companies that profit from the sending of such communications. Cooperation with relevant private sector is essential as well.

As a proactive approach, countries should review periodically their own domestic frameworks and take steps to ensure their effectiveness for cross-border co-operation in the enforcement of applicable laws. In fact, co-operation at the national level would be particularly important to avoid duplication of activities, and allow the optimization of resources and the exploitation of synergies between the different players. In this regard, national legislation could facilitate

information sharing and mutual assistance between competent authorities in different countries through bilateral and/or multilateral agreements and by participating in international bodies and enforcement cooperation initiatives such as London Action Plan (LAP), OECD and ITU.

Industry driven initiatives

Industry driven initiatives, or self regulatory activities, are activities initiated by the industry, either being imposed by the local enforcement authorities, or when there is a need for the industry to take some action against SPAMming activities. Private sector players such as ISPs, telecommunications operators, and direct marketers, play a critical role in the fight against SPAM. In fact, all the countries involved in the battle against SPAM have coupled their anti-SPAM laws with self-regulatory initiatives mainly through the development of codes of conduct for ISPs and e-marketers and making these codes either binding or voluntary. Other form of industry assistance is reflected in awareness programs, software products, sharing information, etc. In this context, OECD and ITU urge industries, including service providers, direct marketers, and software makers to adopt best practices in order to combat SPAM. In particular, Governments and regulators should support the development of codes of practice for electronic marketing and ISPs. Moreover, improved cooperation on enforcement between industry and enforcement authorities should also be promoted.

For instance, in the USA, ISPs include anti-SPAM clauses in their Acceptable Use Policy (AUP). Another example is the GSM Association (GSMA) and the Mobile Marketing Association (MMA) which developed a Mobile SPAM Code of Practice where mobile operators commit to include anti-spam conditions with all new contracts and provide a mechanism to ensure appropriate customer consent and control with respect to mobile operators' own marketing communications.

Technical solutions

Although legislation, government action and industry assistance are fundamental, solutions to eliminating SPAM need to be supported by appropriate technical measures. Anti-SPAM tools that operate at different levels together, with the proper administration and monitoring, make up the technical solutions to SPAM.

In this regard, OECD believes that judicious application of technology should be the backbone of any approach that aims to defeat SPAM. Indeed, none of the technologies acts as a "silver bullet" or one-stop solution to the problems created by SPAM; instead, all of the technologies are complementary and will be most effective when implemented in conjunction with each other. It is recommended that Internet Service Providers and other network operators should constantly improve their knowledge and operating practices, and update their technical best practices in order to face new challenges and technological evolution and promote the implementation and sharing of available technical solutions among providers.

There are different anti-Spam technologies that are used to fight Spam. Typically, anti-SPAM technologies can be based on filters, authentication, and blacklists/white lists which might be augmented to filters. These technologies can be deployed at the client side or the gateway. According to ITU and OECD, each of the available technologies has its weaknesses and strengths and the integration of a number of technologies is crucial to reduce the impact of SPAM.

Education and awareness

Increasing education and awareness is a crucial part of a comprehensive anti-SPAM strategy. Simply, one of the reasons why SPAMmers are successful is that some e-mail recipients are

still responding to SPAM and purchasing advertised products or services, visiting websites advertised by SPAMmers, or being tricked into responding to requests for personal information from 'phishing' scams.

SPAM awareness programs might be sponsored by different entities such as SPAM law enforcement agencies, governmental and non-governmental organizations. They should target different stakeholders such as end users, ISPs and e-marketers. Moreover, it might take different forms such as creating Web sites, hosting SPAM-related conferences, releasing guidelines and best practices, and others.

According to OECD, SPAM awareness and education should target students, children, individuals, Internet Service Providers (ISPs) and Email Service Providers (ESPs), business entities, especially small and medium enterprises (SMEs) and recommends that governments, direct marketers, user's groups, large companies and SMEs, and industry corporations should launch awareness programs.

Governments, as per ITU recommendations, should make sure that consumers are aware of where they can complain, what will be investigated, what action may be taken, and what information they need for authorities to launch an investigation.

SPAM Measurement

SPAM measurements are the ways used to report the effectiveness of the SPAM solutions being deployed to combat SPAM. Measurement is very critical to evaluating the evolution of SPAM and the efficacy of anti-SPAM solutions and educational efforts, to be able to determine if a strategy is effective, and eventually what changes are needed in policy, regulatory and technical frameworks.

In this regard, OECD mentions that:

- Governments and private sector players should monitor the impact of anti-SPAM measures, to assess their effectiveness.
- ISPs, other network operators, and national anti-SPAM agencies should, to the extent possible, share information and data on the intensity and scope of SPAM and its evolution.
- Measuring methods should be detailed and documented, in order to improve the legibility of the results obtained.

Ideally, government and private sector monitor the impact of anti-SPAM measures. Several firms provide mechanisms to collect statistics which is used ultimately to describe SPAM such as the Messaging Anti-Abuse Working Group (MAAWG) email metrics program which is used by the authorities in different countries.

International Cooperation and Exchange

Global co-operation is fundamental to promote appropriate domestic frameworks to counter SPAM in all countries, and to encourage co-operation among governments, private sector, civil society and other stakeholders, in order to ensure the harmonized and widespread application of technical measures and the effective enforcement of applicable rules. Countries involved in the battle against SPAM consider International cooperation as one of the pillars of the anti-SPAM framework. It contributes significantly in the fields of laws and regulations, enforcement, education and awareness and industry cooperation.

The international cooperation takes different forms through cooperating with regional and international entities, signing agreements, entering into MoUs, belonging to international

bodies fighting against SPAM, sharing knowledge and raising awareness, and developing international industry codes and guidelines. In fact, and due to its importance of the global cooperation in the battle against SPAM, OECD recommends that:

- National co-ordination should be first priority;
- Cross-border enforcement against SPAM requires a global strategy to reach effectiveness;
- There has to be strategy in place that handles and organizes SPAM matters from around the world;
- Global outreach should be the objective;
- Action must be taken against SPAMmers no matter where they are, and hence, a reach out to the broadest possible coalition of enforcement agencies worldwide is needed;
- Adequate mechanisms for information gathering and sharing are needed for enforcement agencies to be able to investigate, preserve and obtain information and evidence and share that information with foreign counterparts in appropriate circumstances; and
- While informal frameworks (bilateral MoUs, multilateral or model MoUs, networks such as the London Action Plan) do indeed improve communication and working-level collaboration, a formal framework may be more appropriate to create a common stable and effective mechanism at global level.

Other international bodies have participated in the international cooperation by making proposals for action, as appropriate, on the governance of Internet as with the Working Group on Internet Governance (WGIG) or by developing set of characteristics to be considered in a code of conduct as an international initiative for all messaging providers as with the Messaging anti-abuse working group (MAAWG).

The problem of spam is complex, and a multi-stakeholder and multi-pronged strategy is fundamental. Developing an anti-SPAM framework is a multi-faceted battle that spans law, enforcement, industry assistance, technology, education and awareness, SPAM measurement, and international cooperation.

The anti-SPAM framework must take into consideration the legal, cultural and environmental aspects, be reviewed periodically, and should seek harmonisation with the international trends in the world to avoid cross-border problems and conflicts with other frameworks adopted in other regimes.