

ANTI-SPAM FRAMEWORKS IN DIFFERENT REGIMES

INTRODUCTION

There are a number of countries that have already implemented anti-SPAM policy frameworks, including legislations, such as Australia, Austria, Belgium, United Kingdom, United States and others. A number of other countries, such as Brazil, Argentina, Canada, Armenia, and Bulgaria, use alternative laws, such as Data Protection laws or Consumer Protection laws to address SPAM issues.

Salient practices adopted among these countries within each of these components are summarized below.

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. According to OECD, national anti-SPAM regulation should attempt to:

- o Preserve the benefits of electronic communications
- o Prohibit and take action against the act of SPAMming, as defined by national law, and
- o Reduce the amount of SPAM.

As the legal, political and cultural environments of different countries vary, neither is a uniform approach used to draft SPAM legislations across countries, nor is a common definition of SPAM accepted at the international level. While most countries have enacted SPAM-specific laws, some countries decided instead to amend and harmonize their existing laws. Even among those having SPAM-specific laws, the implementation of the regulatory elements varies significantly between countries.

The scope of applicability of the SPAM legislation is the first element to clarify in the regulatory framework. The legislative definition of SPAM may focus on a particular messaging medium, i.e. technology-based where specific technologies are addressed, or provides a long-term technology neutral approach that provides an overarching statement of principles that are more broadly applicable. OECD states clearly that new legislation should be sufficiently flexible to ensure that communication technologies are covered in the event that they are subject to new forms of SPAM. In fact, restricting the scope of the legislation to a certain technology means that it will be necessary to update laws regularly to face new threats and cover new emerging technologies and applications.

For instance, the “CAN SPAM Act of 2003”, in the US, uses a technology-based approach that is explicitly focused on dealing with electronic mail. It regulates interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet. Fax SPAM and SMS SPAM are addressed through two other separate laws.

Apart from the technology specific nature of the SPAM, legislations also frequently address the content of the SPAM message. Since the majority of SPAMmers aim at making money through the sale of goods or services or through some sort of fraud, legislators are faced with the dilemma of whether the anti-SPAM legislation should only address commercial messages, or also address non-commercial content, such as political or religious messages. For instance, the anti-SPAM legislations in the US and Australia focus only on commercial communications as per their definition of SPAM.. However, according to OECD, limiting the scope of SPAM legislation to commercial messages only may lead to overlooking equally harmful types of SPAM. A million SPAM messages promoting political or misleading religious ideas can be as disturbing as a million messages promoting drugs and goods. Defining the nature of prohibited

messages can be coupled with exemptions from legislation in certain instances. For instance, in most of the countries, communications such as those between governments and citizens, as well as appeals for donations by charities and religious organizations are excluded from the application of the law.

A fundamental principle used in formulating most anti-SPAM policy frameworks is based on ensuring that suitable consent shall be obtained from potential message recipients before sending commercial messages. A number of conceptual frameworks have been utilized in relation to consent, including opt-in and opt-out models. Recent approaches to SPAM regulation have incorporated more complex or subtle methods involving express consent, inferred consent, implied consent, assumed consent or a blend of these. According to OECD, more complex approaches to consent can increase the difficulty of drafting the legislation, but can also assist in creating an approach which attracts the support of both anti-SPAM advocacy groups and direct marketing organizations. For example, Australia, United Kingdom, Belgium, and Malaysia address SPAM through an opt-in approach where transmitting of unsolicited messages is prohibited unless recipients previously consented to receive messages from the sender. On the other hand, USA and Korea have adopted the Opt-out approach for email only where the SPAM law operates on the basis that there is already an assumed consent unless it is at a later stage cancelled by the receiver.

Since legitimate messages are sent through the same messaging media as SPAM, according to OECD, there are two choices when developing a regulatory response:

- o To define classifications of messages based on technology, sender or content that will not be touched by the regulatory regime – that are outside of its coverage.
- o To establish rules of practice that may be followed in order to be considered legitimate messages.

The requirements for legitimate messages are defined through the following elements:

- o Unsubscribe option;
- o Message origin;
- o Bulk; and
- o Labelling.

Some countries have chosen to use labelling to identify the content of the message and to allow users to distinguish between advertising and other personal and professional e-mail. For instance, the Korean legislation includes strict labelling requirements for legitimate advertisement messages. The sender is required to expressly indicate the objective of transmission and major contents thereof “ADV” (for advertisement) or “ADLT” (for adult content) must be included in headers wherever relevant. USA, Singapore and Peru SPAM legislations require labelling while in Australia and Canada there is no labelling requirement within their laws.

SPAM regulators might choose to address the pre-activities for SPAMmers; the ancillary elements that mainly include the utilization of software that harvests contact details and e-mail addresses from the Internet. It covers also the generation of random addressees (Dictionary attacks) where SPAM messages will be sent. According to OECD, the legislation may include specific provisions to levy additional sanctions if such tools are used to aid the sending of SPAM in contravention of the jurisdiction’s SPAM legislation. In fact, many countries have addressed those ancillary elements (such as Australia, Korea, Canada and Singapore). They prohibit supplying, acquiring or using electronic address-harvesting software or lists which have been generated using such software for the purpose of sending unsolicited commercial electronic messages.

Although SPAM in itself constitutes an abuse, SPAM messages include malicious content as well. The decision as to whether this should be addressed by the anti-SPAM regulatory regime is

best decided with reference to the national circumstances. It should be recognized, however, that in many countries the malware aspect of SPAM is criminalized by statute or can be readily criminalized using the Council of Europe Convention on Cybercrime framework.

SPAM legislation may be drafted to require that goods and services advertised and/or offered in messages must be legal, accurately described and commercially responsible. It might as well target criminal or pornographic messages whether by making it part of the jurisdiction's definition of SPAM, associating additional penalties to messages containing these elements, or by requiring additional measures of compliance where possible.

In this regard, OECD clarifies that legislation should:

- o Forbid the unauthorized use of protected computer resources and anybody compromising computers in order to use them to send messages should be sanctioned.
- o Include provisions on prohibiting misleading or deceptive subject heading and may cover the content of messages, in particular if anti-fraud laws, consumer protection legislation, etc. are not clearly drawn out.

Finally, it is difficult to impose legislation on SPAM messages that have originated outside the jurisdiction of the recipient's country. At the same time, countries do not always have legal jurisdiction over SPAM messages that originate within their borders but are sent to a different country. Factors that might affect the cross-border jurisdiction are the limitation in the SPAM law itself and the insufficient international cooperation and cross-border enforcement agreements. Moreover, in many instances, one part of the evidence for a case is in another country, as happens for example in the case of investigations regarding banks accounts, intermediary companies, hosting companies, etc.

ENFORCEMENT COOPERATION

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.

The main purpose of enforcement and sanctions is to:

- o Ensure that compliance to defined legitimate messaging behaviours is mandatory rather than voluntary, and
- o To impose financial or other costs on SPAMmers, lessening or removing the profits received from illicit activities, and therefore the motivation to undertake SPAMming activity.

This component, enforcement cooperation, describes the enforcement agencies, their inter-cooperation, how they handle complaints, the different types of sanctions and how they are applied, and finally the nature and extent of the powers they possess for enforcing laws that are used to take action against SPAMmers.

It is common to see the responsibility for SPAM scattered across multiple agencies. This is based on the variety of abuses committed through electronic communications, and the fact that violations conducted by SPAMmers touch upon different laws such as the consumer protection laws, criminal laws, data protection laws, and telecommunication laws. In the vast majority of countries, whether having anti-SPAM specific law or relying on other existing laws, enforcement of the various applicable laws falls within the jurisdiction of several agencies. For instance, in Canada, the Competition Bureau has the power to initiate proceedings against SPAMmers if commercial representations contained in an e-mail are false or misleading, whereas the Privacy Commissioner may take action in cases where personal information, such as an e-mail address, is used without the consent of the data subject. Another example is the USA, where three enforcement agencies are responsible for the enforcement of the CAN SPAM Act, while four enforcement agencies are responsible for the enforcement in Australia. Even though several

agencies may be dealing with SPAM in the same country, ideally, there is a specific authority which takes the lead, and puts more effort and resources in the fight against SPAMmers and plays an important role at both national and international levels, functioning as a point of contact and participating in international activities. For example, the FTC, which has a larger role in the field than the FCC, deals principally with mobile SPAM.

Having multiple agencies in place raises the question specifically asked whether each country has any protocols or arrangements in place to refer complaints about SPAM or share information between agencies of the coordination and cooperation required between the different enforcement agencies. In fact, just few countries have protocols at the national level for these purposes. Other countries have informal intra-agency co-operation which occurs without any agreed-upon protocol. This is the case for example of Belgium, where co-operation among different authorities is informal. On the other hand, the USA and Australia provide a national coordinated approach to combat complex and multi-jurisdictional crimes, especially those beyond the capability of single jurisdictions.

In this regard, OECD recommends that:

- o Countries need to increase efforts to strengthen domestic inter-agency co-operation.
- o One agency is assigned as a contact point for foreign authorities to facilitate cross border co-operation.
- o 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.

The first phase of anti-SPAM law enforcement involves receiving complaints about SPAM from users. This requires communication with the recipients of SPAM and the operators of networks through which it is sent. A framework for handling complaints has been developed by all countries involved in the fight against SPAM. All agencies with responsibility for enforcing a SPAM-related law provide at least one means for recipients to notify the authority concerned, which may include sending the complaint through e-mail, filling out a form on the agency's web site, telephone, fax or post. In a few cases, as in the UK and Australia, the enforcement agency provides an online complaint form, which is perhaps the most efficient means to collect complaints and evidence.

Law enforcement agencies often distinguish between professional SPAMmers and legitimate businesses that have overlooked the law. In Australia, the Australian Communications Authority (ACA) has sent 150 warning letters to businesses when the SPAM Act was enacted in April 2004, but its policy is to reserve fines for professional SPAMmers, which include those that send hundreds of thousands of e-mails marketing fraudulent goods and services and businesses that repeatedly violate the SPAM Act.

After receiving a complaint, one of the greatest challenges facing enforcement agencies is the identification of the source of SPAM and gathering evidence to link a specific person to the act of sending SPAM. Consequently, enforcement agencies require the tools necessary to obtain sufficient and acceptable evidence for investigations to proceed to the sanctioning phase of enforcement. More obstacles and issues confront enforcement agencies that wish to co-operate at the international level with foreign counterparts in taking action against SPAMmers located in other countries. To address this international issue, most countries seek cooperation 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. Moreover, OECD recommends setting priorities regarding what types of complaints are most appropriate for cross border co-operation.

The majority of the agencies possess the power to compel production of documentary evidence and witness testimony, and to conduct on-site inspections at businesses. For instance, the Australian Communications Authority (ACA) can request that information be provided

voluntarily; compel any person to provide information, with criminal or civil penalties available for non-compliance; obtain a warrant issued by the court to search and seize; obtain an ongoing monitoring warrant for persons who have signed enforceable undertakings, or where the federal court has found that an individual has breached the Act; and subpoena evidence. The Canadian Competition Bureau can ask for voluntary provision of information/evidence and can apply to a court to obtain various orders for the production of records and written returns of information and for individuals to be examined under oath or solemn affirmation. According to OECD, enforcement authorities dealing with illegal SPAM need appropriate search and seizure powers to preserve, access, intercept, search and seize electronic evidence.

Once a complaint about SPAM has been reported to the appropriate enforcement agency and the investigation has been conducted, the next phase of enforcement is to initiate an action which might vary from administrative action, civil proceedings, and criminal proceedings. OECD recommends that legislation needs to foresee sanctions severe enough to discourage SPAM by cutting into the profit or foreseeing criminal sanctions such as detention for certain violations. The tools available to enforcement agencies in the fight against SPAM range from the soft coercion of warning letters to the deprivation of liberty through imprisonment. In fact, the two most widely available non-monetary remedies are warning letters and injunctions. For instance, violators of the US CAN-SPAM Act can be fined up to US 250 per violation, to a cap of US 2 million, for non-willful and non-compliance; and up to US 6 million for intentional violations, plus unlimited punitive damages for fraud and abuse. In the most severe cases, prison sentences of up to five years are available as penalties. In Korea, the most common sanctions are fines, these usually fall into the range of 1 to 7 million Korean Won. If the case is not that severe, the court may order the offending entity to pay compensations for the damage caused. In some cases, however, depending on severity, failing to abide to the rules might even result in some legal action against the offenders that could lead to landing some jail time.

Enforcement agencies face significant obstacles in carrying out their duties, due to the difficulty and expense incurred to track down SPAMmers and gather sufficient evidence to prosecute them and recovering monetary rewards for victims. Moreover, to effectively curb SPAM, the timeliness and speed with which investigations are conducted and sanctions are applied is crucial. Traditional enforcement approaches which take weeks or months will not be effective in the online world.

INDUSTRY DRIVEN INITIATIVES

Industry driven initiatives, or self regulatory activities, are activities initiated by the industry, either through 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, In fact, OECD recommends that:

- o Governments and regulators should support the development of ISP codes of practice that complement and are consistent with legislation. Moreover, governments should encourage industry associations to develop such codes and adopt best practices where they are in the public interest and do not impose undue financial and administrative burdens on participants.
- o ISPs should be able to take appropriate and balanced defensive measures to protect their networks, and should be allowed to take legal action against SPAMmers. Similar results could be achieved through appropriate contractual provisions between ISPs and users.

- o "More effective approach" would be to mandate establishment of enforceable codes of conduct by internet service providers, which would be held responsible for SPAM from their customers. Those codes would require ISPs to prohibit their customers from SPAMming and not to enter into peering arrangements with ISPs that do not accept similar codes of conduct.
- o Direct Marketers should adopt and effectively implement a code of conduct using best practices for electronic marketing, which include marketing messages sent by e-mail, instant messaging, or mobile.

The codes of conduct give practical guidelines and set a framework for dealing with complaints. 'Don't Fax' and 'Don't Email' services are examples of industry taken initiative which creates a list of customers who don't want to receive emails or faxes. Industry support and assistance was established in all countries, for instance:

- o In the USA, ISPs include anti-SPAM clauses in their Acceptable Use Policy (AUP) which impact directly their customers and the Federal Trade Commission (FTC) has published several documents targeted at eMarketers/Commercial Emailers.
- o The Australian Telecommunications Act 1997 sets out the intention of the Commonwealth Parliament that bodies and associations in the telecommunications industry develop industry codes relating to the telecommunications activities of those bodies. In fact, the Direct Marketing Association has developed eMarketing Code of Practice and the Internet Industry Association and a taskforce developed a code of conduct for Internet and email service providers (ISPs). Moreover, two more codes of conduct were developed for fax and SMS.
- o In Singapore, an anti-SPAM website, named the "Singapore Anti-SPAM Resource Centre" has been launched to provide a central anti-SPAM repository for the public and industry. This website was jointly developed by various industries.

TECHNICAL SOLUTION

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 recommends that:

- o Judicious application of technology should be the backbone of any approach that aims to defeat SPAM.
- o That none of the technologies will act as a "silver bullet" or one-stop solution to the problems created by SPAM.
- o All of the technologies are complementary and will be most effective when implemented in conjunction with each other.
- o The integration of a number of technologies is necessary to reduce the harmful impact of SPAM on a system.
- o 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.

In fact, experiences of various countries show that laws, regulations, and industry assistance are not sufficient, without technical solutions, to eliminate SPAM. Anti-SPAM technological tools are typically implemented all the way from where the SPAM message originates to the end where it gets received. Information regarding anti-SPAM tools is kept confidential as publishing such information might help SPAMmers to defeat such measures.

EDUCATION AND AWARENESS INITIATIVES

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 might 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 student, children, individuals, ISPs/ESPs, business entities, especially SMEs and recommends that governments, direct marketers, user's groups, large companies and SMEs, and industry corporations should launch awareness programs.

In Australia, for instance, the Australian Direct Marketing Association (ADMA) raises awareness in the marketing arena and offers education and certificates. In the USA, the Government sector represented by the Federal Trade Commission (FTC) for example, has developed a website about SPAM in both English & Spanish language. It provides the most current information, as well as interactive features, such as videos and quizzes. The FTC also has conducted high-profile education and awareness-raising campaigns on such topics as recognizing scams on the Internet, shopping securely online, avoiding hackers and viruses, and dealing with SPAM, spyware, phishing and ID theft.

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 effectiveness 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:

- o Governments and private sector players should monitor the impact of anti-SPAM measures, to assess their effectiveness.
- o 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.
- o 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 the USA. Singapore, to understand the nature and extent of e-mail SPAM, a survey on unsolicited e-mails was conducted as an ad-hoc survey commissioned by IDA and Precision Research in October 2003.

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:

- o National co-ordination should be first priority;
- o Cross-border enforcement against SPAM requires a global strategy to reach effectiveness;
- o There has to be strategy in place that handles and organizes SPAM matters from around the world;
- o Global outreach should be the objective;
- o 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;
- o 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
- o 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.

All the countries involved in the fight against SPAM have been cooperating on the international level. For example, to extend Singapore's anti-SPAM efforts to international shores, IDA participated in the US Federal Trade Commission's "Operation Secure Your Server" campaign, to encourage organizations worldwide to close open relays and proxies in January this year. IDA is also committed to participate in international initiatives, including participation in global and regional fora such as APEC, ITU, OECD and ASEAN.

Another example is Canada. With the support of the Task Force, the Industries in Canada and the Department of Foreign Affairs have developed and are negotiating a series of bilateral agreements between Canada and the United Kingdom, Australia, the United States and the European Commission. Agreements with the United Kingdom and Australia will be ready for approval within the next two months.