RESEARCH REPORT

"Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in the Asia-Pacific Region"

Edition: June 2024

Korea Internet & Security Agency

Asia-Pacific Telecommunity (APT) is the only intergovernmental organization specialized in the ICT field in the Asia-Pacific region, established in 1979 by the joint initiatives of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) and the International Telecommunication Union (ITU) with the objective of fostering the development of telecommunication services and data infrastructure throughout the region, particularly focus on developing areas.

Through its various programmes and activities focused on 5 Strategic Pillars as follow, the APT continues to support and assist its 38 Members, 4 Associate Members and 143 Affiliate Members (as of December 2023) to realize the positive benefits of ICTs and cope with the challenges of rapidly evolving ICT environments.

For further information, please visit the APT website at https://www.apt.int.

Strategic Pillars of the APT (Strategic Plan of the APT for 2021-2023)

a. Digital Connectivity: Enhancing access and efficiency of telecommunication/ICT infrastructure, including broadband infrastructure;
b. Digital Transformation: Enabling conducive environment and harnessing the benefits of telecommunication/ICT;
c. Trust and Safety: Ensuring secure cyberspace, security and resilience through telecommunication/ICT;
d. Digital Inclusion: Removing barriers to promote digital inclusiveness;
e. Sustainability: Broadening participation in the telecommunication/ICT sector, and using ICTs to adapt to climate change and mitigate its impact

Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in the Asia Pacific Region

Period: March to December 2023

Asia Pacific Telecommunity (APT)

Sun Kyung Choi
Programme Officer

Shreya Pradhan
Assistant Project Coordinator

Korea Internet & Security Agency (KISA)

Jung Eu An
Manager

Kyeongsik Park
General Researcher

Executive Summary

The APT has focused on implementing its Strategic Plan 2021-2023 adopted by the 15th Session of General Assembly of the APT (GA-15) enumerates five strategic pillars and "Trust and Safety" is one of them. The strategic direction of this pillar is "to develop and maintain secure, trusted and resilient telecommunication/ICT networks and services". Accordingly, the 44th, 45th and 46th session of the Management Committee (MC-44, MC-45, MC-46) of the APT from 2020 to 2022 respectively approved to conduct research on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia Pacific Region" (MC44/OUT-18, MC45/OUT-09, MC46/OUT-15).

While several studies on unsolicited commercial messages have been conducted in recent years, including by the ITU and other international cooperation initiatives, there has been a lack of relevant and up-to-date information on the status of APT Members regarding unsolicited commercial messages in the Asia-Pacific region. In recognition of this, the APT-KISA joint study has been conducting surveys over the past two years to understand the current status of spam-related issues, laws, and policies in member countries. As a result, we have been able to compile the current status of spam-related laws and policies in 25 Members, which provides a basis for examining ways to mitigate the negative impact of spam. The study is significant in that it laid the foundation for sharing global and regional best practices and policy experiences among APT Members and facilitating policy/regulation formation.

The final goal of this research project is to find collaborative response measures to prevent unsolicited commercial messages in the Asia-Pacific region. Therefore, this year, based on the survey results in 25 Members, the research team has conducted a more detailed desk study in order to identify common factors in the policies of each Members and recommend countermeasures for the development of advanced anti-spam policies. The purpose was to provide a co-operative framework for a joint response by highlighting the need for an international response to spam, while enabling Member States to utilize it in their own policy formulation.

Legal Framework

According to the survey results, spam emails and SMS/MMS (hereinafter referred to as spam messages) are regulated by the laws in most Members replied to the survey. However, it can be divided into cases where separate laws are enacted specifically for them and cases where provisions related to them are stipulated in ICT-related laws.

In terms of regulating spam emails, 9 of the 25 Members surveyed (Australia, Cook Islands, Republic of Korea, Japan, Singapore, China, New Zealand, Hong Kong, and Vietnam) have comprehensive spam legislation. With regard to the spam messages, 9 Members (Australia, Cook Islands, South Korea, Japan, Singapore, New Zealand, Hong Kon, Philippines, and

Vietnam) have comprehensive legislation against them.

Regarding the Authorities, it has been observed that in most Members, policy bodies in the ICT sector are tasked with this responsibility. The form of these responsible Authorities varies, ranging from independent ministries to agencies or organizations under the Prime Minister's Office. In most Members, it has been found that these regulatory Authorities are responsible for formulating the spam related policies, executing them, and taking actions in case of violations. x

Regulatory Approaches

We have identified various regulatory approaches to restrict spam emails/messages, such as opt-in/out scheme, prior consent requirement, unsubscribe facility, labeling obligation, and prohibit of the address harvesting Software. However, it was reaffirmed that the operation and content of these systems may vary depending on the economic and social environment of the Members, the nature of the regulator, and differences in perceptions of spam, etc.

Additionally, it is noteworthy that a majority of Members have shifted towards direct regulation over reliance on self-regulation by private entities. This indicates that solely relying on self-regulation is insufficient in curtailing spam, suggesting that a blend of self-regulation and governmental oversight might offer the most potent solution. Nevertheless, any spam control legislation or policy should be adaptable to accommodate the unique circumstances of each Member. By drawing from the diverse examples explored in this research, each Member can devise suitable legislation or policies.

Non-Regulatory Approaches

The results from a three-year survey also show that Members' anti-spam policies include both regulatory and non-regulatory approaches. Non-regulatory approaches range from supporting technical measures, self-regulation, education and awareness-raising activities, and international cooperation activities, and Members have developed the spam policies based on their own circumstances.

While the survey results provide some indication that Members are undertaking some activities for technical measures, self-regulation or awareness-raising, additional work is needed to confirm the specifics and linkages with other activities to ensure a safe ICT environment. However, further efforts are encouraged to build the foundations for safe network use through non-regulatory approaches in partnership with governments and the private sector, given the enforcement limitations of regulatory approaches.

Way Forward

The three-year spam policy survey provided a comprehensive overview of the current state of

spam response across Members. It scrutinized the effectiveness and scope of various policies, highlighting strengths and weakness, and included a comparative analysis among Members. Based on responses from 25 members, the survey aims to identify best practices and lay the groundwork for enhancing spam response mechanisms.

However, certain trends remain unidentified, and future research will delve deeper into the nuances of anti-spam strategies. This includes examining non-regulatory approaches like technical measures, self-regulation, and awareness-raising efforts. As exploration of multi-pronged approaches will be crucial in developing effective global responses to the evolving spam issues.

Contents

1. Introduction

1.1 Background

The APT-KISA Joint Research Initiative is a collaborative effort to address the problem of unsolicited commercial messages, commonly referred to as spam, that is prevalent in the Asia-Pacific region. Spam poses a multi-faceted threat to electronic communications platforms and services as it can deceive users, disrupt networks, and facilitate the spread of various forms of fraud and malware.

Given the critical nature of this problem, the Strategic Plan of the APT for 2021-2023, ratified during the 15th Session of General Assembly (GA-15), identifies "Trust and Safety" as one of its five strategic pillars. Within this framework, the objective is clear: to foster secure, trusted, and resilient telecommunication and ICT networks and services.

To realize this objective, the 44th session of the Management Committee (MC-44) of the APT, held in 2020, approved a comprehensive research endeavor titled "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia Pacific Region" (MC44/OUT-18). The research initiative was jointly conducted by the APT and the Korea Internet & Security Agency (KISA), Republic of Korea from 2021 to 2023.

The initiative aims to comprehensively identify and analyse the general landscape of spam-related issues, laws, and policies across APT member countries, including data collection on existing legal and regulatory frameworks regulating spam, spam suppression activities of private telecommunications companies, and cross-border cooperation activities. By facilitating the sharing of global and regional best practices and policy experiences among APT members, the study aims to strengthen our collective understanding and capacity to effectively address spam.

Ultimately, the insights gained from this study will contribute to informing the policy and regulatory formulation process within APT member countries. In other words, through this study, the APT aims to provide a range of frameworks that can be adapted to the policy environment of each country to prevent and combat the adverse effects of spam. In doing so, the APT aims to ensure trust, stability, and resilience of electronic communications networks and services in the Asia-Pacific region through a proactive and collaborative approach, while contributing to the broader goals of economic and social development in the region.

1.2 Research method

As part of our initial efforts to comprehensively assess and analyse members' spam-related legislative and policy frameworks, we conducted a survey to gather accurate policy data and insights, then undertook a desk study based on the data collected to further strengthen our analysis.

Survey Questionnaire

In the initial approach, a questionnaire developed in collaboration with KISA was distributed to APT members, designed to elicit responses regarding existing spam legislation, policy frameworks, enforcement strategies, and ongoing private sector efforts to mitigate spam within each member's jurisdiction. In particular, the survey was conducted to determine whether spam legislation has the following spam regulatory factors: opt-in/out scheme, prior consent, unsubscribe facility, sender information, bulk sending, and labeling obligations.

A total of 25 members participated in the survey between 2021 and 2023. We used this dataset to examine the legal regulatory framework of these members across the various factors described above. This allowed for comparative analysis across members to identify patterns, changes, and trends in the regulatory environment related to spam.

This collaborative initiative aimed to facilitate direct interaction with APT members to gain accurate and detailed insights into the spam regulatory environment in various countries. This approach enabled comprehensive data collection that accurately reflected the unique circumstances and context of individual members.

Desk Study

The second method entails conducting a desk study to complement the survey responses and gather additional insights. This involves researching legislative cases of countries that are actively pursuing or promoting the enactment or revision of spam-related laws, as well as analyzing policy documents and relevant information available on the web. By leveraging publicly available data and resources, such as official government websites, legal databases, and academic publications, the initiative can enrich its understanding of the broader policy landscape and emerging trends in spam regulation across the region. This method allows for cross-referencing and validation of information obtained through the survey, ensuring a more comprehensive and accurate assessment.

By running these two approaches in parallel, the initiative benefits from a synergistic combination of qualitative and quantitative data sources. The survey questionnaire provides direct insights from APT Members, while the desk study offers broader context and

supplementary information. This integrated approach enhances the accuracy and reliability of the findings, enabling a thorough understanding of individual countries' spam legislation and policy schemes within the Asia-Pacific region. Ultimately, this comprehensive analysis serves as a valuable foundation for informing collaborative response measures to prevent unsolicited commercial messages and strengthen trust and safety in electronic communication networks and services.

2. Regulatory Approaches

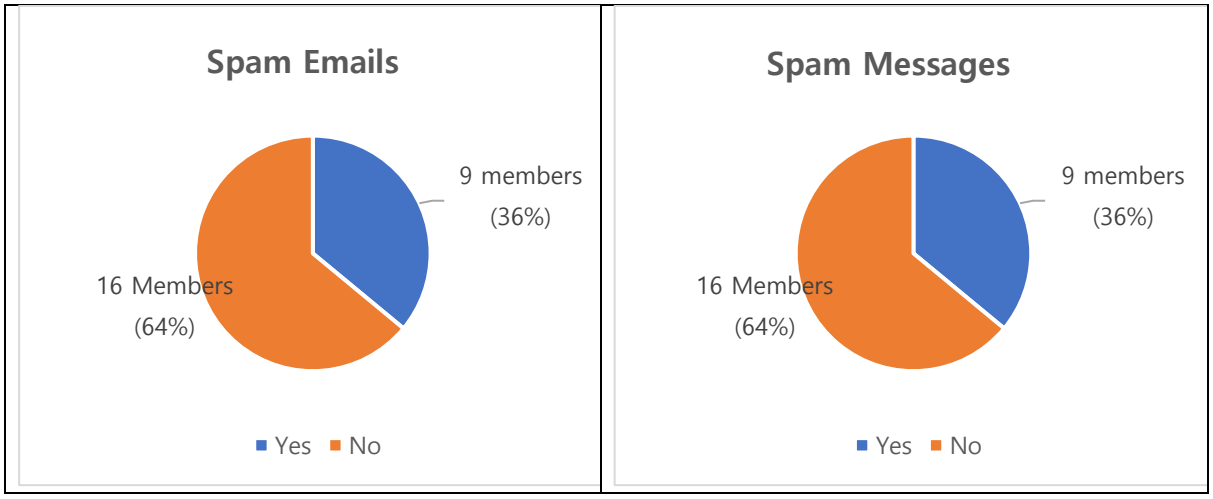
2.1. Legal Framework

In this section, we identify how Members have developed a legal regulatory framework for unsolicited(spam) emails and messages, which will provide a basis for comparison between Members, as well as suggestions for further development of the legal framework.

In general, legislation to regulate spam follows two approaches. The first approach is to create separate and specific legislation to regulate spam emails and messages. The second approach is to address spam-related issues within the existing legal framework (i.e., consumer protection, cybercrime, network security, etc.).

The survey asked about the existence of comprehensive anti-spam legislation and the results showed that of the 25 countries that responded to the survey, 9 members have comprehensive legislation anti-spam legislation and 9 members have anti-spam legislation. Other countries have spam-related provisions in their cybercrime or network security laws.

APT Members' Anti-Spam Legislation



Of the 25 members who responded to the survey, 9 members have spam legislation, representing 36% of all responding members, but the percentage of APT members with spam legislation is likely to be lower if we include members who did not respond to the survey.

APT Members' Anti-Spam Legislation

Members	Spam Emails	Spam Messages (SMS/MMS)
Australia	The Spam Act 2003	
Cook Islands	The Spam Act 2008	
Republic of Korea	The Information and Communications Network Act	
Japan	The Anti-Spam Act	
Singapore	The Spam Control Act	
P.R. China	The Regulation for the Administration of Internet email Services	-
New Zealand	The Unsolicited Electronic Messages Act 2007	
Hong Kong	The Unsolicited Electronic Message Ordinance	
Philippines	-	The Public Telecommunication Services Act
Vietnam	The Enforcement Decree of the Law on Information Technology	

As can be seen from the table above, Australia, Cook Islands, Japan, Singapore, New Zealand, and Hong Kong have enacted separate spam email/message laws. South Korea does not have a separate spam email/messaging law but has a separate provision on spam in the Information and Communications Network Act to specifically and systematically regulate spam email/messaging. P.R. China has a separate administrative regulation on spam emails, and Philippines has enacted a separate administrative regulation to regulate spam messages. Vietnam has enacted an implementing decree to comprehensively regulate spam emails/messages.

Spam emails

With regards to spam email, 9 members out of the 25 members (Australia, Cook Islands, Republic of Korea, Japan, Singapore, People's Republic of China, New Zealand, Hong Kong, and Vietnam) have comprehensive spam legislation and a well-established regulatory framework to protect users from spam. Six members (Australia, Cook Islands, Japan, Singapore, New Zealand, and Hong Kong) have enacted separate spam laws. South Korea does not have separate spam legislation, however, specifically, and systematically regulates spam

emails through separate provisions in the Information and Communications Network Act. The P.R. China has a separate administrative regulation on spam, and Vietnam comprehensively regulates spam through an implementing Decree.

Thailand, Pakistan, and Bhutan do not have a comprehensive legal framework on spam email and regulate spam email through other legislation. Thailand has an opt-in framework through the Computer Crimes Act, which prohibits the sending of emails without an unsubscribe facility, as well as the sending of emails that interfere with the normal use of computer systems. Pakistan also has an opt-in scheme through the Electronic Crimes Act, which prohibits the sending of emails without consent and without an unsubscribe facility. Papua New Guinea regulates spam email under the Cybercrime Code Act. Bhutan has an opt-out scheme to regulate spam emails in the Information and Communication Media Act.

Cambodia, Lao PDR, Malaysia, Nepal, India, Indonesia, Philippines, Brunei Darussalam, Federated States of Micronesia, Kiribati, Tonga, and Sri Lanka have no direct and specific laws, decrees, or administrative regulations against spam email. However, Malaysia, Indonesia, and Kiribati have no direct regulation but regulate spam email indirectly to a certain level. In the case of Malaysia, the Telecommunications and Multimedia Act states that “(1) A person who initiates a communication with the intent to offend or harass another person to a number or electronic address, whether persistent, repetitive, or otherwise, (2) A person who transmits a comment, request, suggestion or other communication of an obscene, inappropriate or offensive nature with the intent to offend or harass” is in breach of the Act.

Indonesia also does not have direct regulations on spam email, but the Internet Law states that "when goods and services are offered for sale through electronic media, the person offering to sell must provide complete and correct information regarding the terms of the contract, the goods and services offered, and the producers of the goods and services."

In the case of Kiribati, the Cybercrime Act 2021 addresses the nature of spam, which in principle relates to unauthorised computer system access or unauthorised computer system interference if spam delivers a malicious payload to a computer system and interferes with its normal operation.

Spam Messages (SMS/MMS)

For those members that have laws that clearly regulate spam, in most cases the same laws also regulate spam messages. 9 Members of the 25 Members surveyed have a comprehensive legal basis for spam messages; Australia, Cook Islands, Republic of Korea, Japan, Singapore, New Zealand, Hong Kong, Vietnam, and Philippines.

Among the other members, Indonesia has enacted a decree to regulate spam SMS in 2021, so it is regulating SMS directly. Pakistan has a regulation system through the Electronic Crimes Act, which prohibits sending SMS without permission and without an unsubscribe facility. In the case of Papua New Guinea, the Cybercrime Code Act is the primary legal basis for

regulating spam messages.

However, 10 members (Cambodia, Lao PDR, Malaysia, Nepal, India, Bhutan, Federal States of Micronesia, Kiribati, Tonga and Sri Lanka) do not have direct or specific legal framework on spam messages. Among them, Malaysia, Nepal, India, and Kiribati regulate spam message to a certain level.

The Telecommunications and Multimedia Act of Malaysia restricts "(1) A person who initiates a communication with the intent to offend or harass another person to a number or electronic address, whether persistent, repetitive, or otherwise, (2) A person who transmits a comment, request, suggestion or other communication of an obscene, inappropriate or offensive nature with the intent to offend or harass". In Kiribati, the Cybercrime Act 2021 in principle covers the nature of spam in relation to unauthorized computer system access to or interference with the computer system, where the spam delivers a malicious payload to a computer system and interferes with its normal operation.

2.2 Authorities

For the most Members, the regulatory Authorities responsible for the regulation of spam emails and messages are the identical, especially those responsible for ICT policy and regulation.

In Singapore, the PDPC (Personal Data Protection Commssion) and the IMDA (Infocomm Media Development Authority) are responsible for dealing with anti-spam policy. Responsibility for managing unsolicited communications falls to the PDPC, which was established to implement the Personal Data Protection Act, and the Info-communications Media development Authority (IMDA), which has responsibility for enacting the Spam Control Act. The PDPC directly enforces the Personal Data Protection Act (covering telephone and fax spam) as it relates to unsolicited communications, and operates do not contact registers for telephone, fax and SMS/MMS. The IMDA has responsibility for the Spam Control Act, though the enforcement of this act happens through a "multi-pronged" approach, including the legislative framework, industry self-regulation, international cooperation and public education.

In New Zealand, the DIA (Department of Internal Affairs) is the Authority responsible for digital safety including anti-spam policy as well as for digital public service, local government, and enterprise partnership.

APT Members' Anti-Spam Regulatory Authorities

Member	Spam Emails	Spam Messages
Australia	ACMA (Australian Communications and Media Authority)	

Bhutan	MIC (Ministry of Information and Communications)	
Korea	KCC (Korea Communications and Commission)	
Japan	MIC (Ministry of Internal Affairs and Communications)	
Singapore	IMDA (Infocomm Media Development Authority) PDPC (Personal Data Protection Commission)	
China	MIIT (Ministry of Industry and Information Technology)	-
Cook Islands	Office of the Prime Minister	
New Zealand	DIA (Department of Internal Affairs)	
Hong Kong	OFCA (Office of the Communications Authority)	
Indonesia	-	MCI (Ministry of Communications and Information)
Thailand	MDES (Ministry of Digital Economy and Society) NBTC (National Broadcasting and Telecommunications Commissions)	-
Pakistan	FIA (Federal Investigation Authority) PTA (Pakistan Telecommunication Authority)	
Papua New Guinea	NICTA (National ICT Authority)	
Philippines	-	NTC (National Telecommunications Commission)
Viet Nam	MIC (Ministry of Information and Communications)	

2.3. Main Elements

In our survey, we explored the main factors of spam regulation: definition of spam, opt-in/out schemes, prior consent, sender information, unsubscribe facilities, labelling obligation and whether address harvesting software is prohibited.

Definition of Spam

There is no agreed-upon definition of spam, and it is defined differently depending on each member's regulatory method. However, members with anti-spam laws show the following common characteristics through their definitions: Electronic/Commercial messages, Hidden or disguised sender, Use of addresses without recipients' consent, and Bulk/repetitive sending.

Many legal definitions of spam emphasize the commercial nature of the message since most spam is created to sell a product or service or to make a profit through scams. In this case, there is no negative impact on freedom of expression because spam does not include personal, political, religious, or ideological messages. However, limiting spam that is regulated to commercial messages has the disadvantage of excluding non-commercial but highly harmful spam.

According to the survey, most Members with anti-spam laws have a clear definition of spam. Generally, they define it as unsolicited advertising electronic messages, with some Members providing more detailed descriptions.

Australia defines that a commercial electronic message is an electronic message were, having regard to the content of the message, the way in which the message is presented, the content that can be located using the links, telephone numbers or contact information (if any) set out in the message: it would be concluded that the purpose, or one or the purposes, of the message is: to offer to supply goods or services; or to advertise or promote goods or services; or to advertise or promote a supplier, or prospective supplier, of goods or services; or to offer to supply land or an interest in land; or to advertise or promote land or an interest in land; or to advertise or promote a supplier, or prospective supplier, of land or an interest in land; or to offer to provide a business opportunity or investment opportunity; or to advertise or promote a business opportunity or investment opportunity; or to advertise or promote a provider, or prospective provider, of a business opportunity or investment opportunity; or to assist or enable a person, by a deception, to dishonestly obtain property belonging to another person; or to assist or enable a person, by a deception, to dishonestly obtain a financial advantage from another person; or to assist or enable a person to dishonestly obtain a gain from another person; or a purpose specified in the regulations.

In the Republic of Korea, spam is defined as "advertisement information for the purpose of profit that is transmitted unilaterally through the information and communication network without the explicit prior consent of the recipient" in the Act on Promotion of Information and Communication Network Utilization and Information Protection.

In Singapore, unsolicited communications or spam refers to emails or text or multimedia messaging to mobile telephone numbers sent in bulk that advertise products and services to a large group of recipients without their prior request or consent.

Even if there are not direct legal framework, it may still regulate spamming behavior by relying on existing laws. In Malaysia, the Communications and Multimedia Act provides that "communications sent to a specific number or electronic address, whether persistent, repetitive, or otherwise, with the intention of offending or harassing another person, or comments, requests, suggestions or other communications sent with an inappropriate and offensive nature and with the intention of offending or harassing another person (Article 233)" as spam.

Papua New Guinea defines that in the Cybercrime Code Act 2016 spam means the transmission of harmful, fraudulent, misleading, illegal, or otherwise unsolicited electronic

messages to a recipient without the express permission or approval of the recipient or causing an electronic system or device to show such message or the involvement in falsified online user account registration or falsified domain name registration, for commercial purpose.

Opt-in vs. Opt-out

Opt-in scheme is an action taken by an individual to actively consent or agree to participate, such as receiving a marketing email, joining a mailing list, or allowing personal information to be collected. It requires an explicit action to indicate consent, such as ticking a box, signing a form, or clicking a button.

By contrast, opt-out scheme is the process of removing oneself from a target, such as a marketing email, or refusing to participate. In marketing, this typically involves giving individuals the option to unsubscribe from emails, newsletters, or other communications. In essence, opt-in means actively choosing to participate, while opt-out means not participating or ceasing to participate.

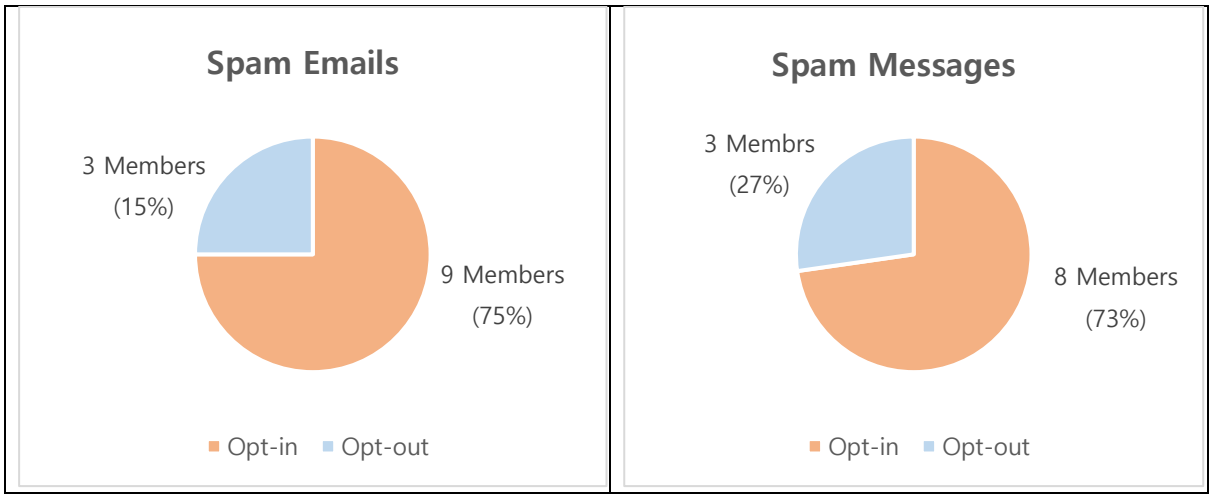
In the case of spam emails, 7 members have adopted the opt-in, and 2 members have adopted the opt-out scheme. Opt-in and opt-out schemes mean that users indicate or withdraw their consent to receive information. Opt-in refers to users consenting to a particular service or information, while opt-out refers to users opting out of receiving a particular service or information.

APT Members' opt-in/opt-out approaches to spam legislation

Member	Spam Emails	Spam Messages
Australia	Opt-in	Opt-in
Bhutan	Opt-out	-
Republic of Korea	Opt-in	Opt-in
Japan	Opt-in	Opt-in
Singapore	Opt-out	Opt-out
P.R. China	Opt-in	-
Cook Islands	Opt-in	Opt-in
New Zealand	Opt-in	Opt-in
Hong Kong	Opt-out	Opt-out
Indonesia	-	Opt-out
Thailand	Opt-in	-
Pakistan	Opt-in	Opt-in

Philippines	-	Opt-in
Viet Nam	Opt-in	Opt-in

APT Members' Opt-in/out Scheme



Members who responded to our survey were applying the same spam schemes to the emails and messages. In the case of spam emails, 9 members (Australia, Republic of Korea, Japan, P.R. China, Cook Islands, New Zealand, Thailand, Pakistan, Viet Nam) adopted an opt-in scheme and 3 members (Bhutan, Singapore, Hong Kong) adopted an opt-out scheme.

For spam messages, 8 members (Australia, Republic of Korea, Japan, Cook Islands, New Zealand, Pakistan, Philippines, Viet Nam) adopted the opt-in method and 3 members (Singapore, Hong Kong, Indonesia) adopted the opt-out scheme.

The Australian government has an opt-in scheme for spam emails and messages and it is illegal to send or cause unsolicited commercial electronic messages to be sent under the Spam Act 2003. It states that the commercial electronic message senders must obtain the recipient's consent, provide the accurate sender information, and include an unsubscribe facility.

Japan has essentially adopted an opt-in scheme for regulating commercial electronic mail and messages, since all the provisions of "Limitation of sending electronic mail" of the Anti-Spam Act require active action by the recipient before the sender is allowed to send commercial electronic mail. Also, when a sender received notice of a request no to send it from any person in accordance with the applicable MIC ordinance, the sender shall not send it against the notifying party's intention indicated in the said notice. There is no grace period for compliance with this request.

In Singapore, which has an opt-out scheme for spam emails, spam messages, and spam phone calls, the Spam Control Act created an opt-out scheme for bulk commercial electronic

messages with Singapore link, email, messages fall within the scope of this system, and message sent via fax or fixed phone numbers, voice calls are not included. Therefore, every unsolicited commercial electronic message shall provide an unsubscribe facility and contain an electronic email address, a telephone number, etc. and where a recipient submits an unsubscribe request using the facility, no further unsolicited commercial electronic messages shall be sent after the expiration of 10 business days after the day on which the unsubscribe request is submitted.

Each member has weighed the pros and cons of opt-in and opt-out system when contemplating its anti-spam policy. In general, the advantages of opt-in approach are that it can reduce the social and economic costs cause the spam emails and messages and that consent-based advertising can be more effectively communicated to consumers. Opt-out approaches have the advantage of encouraging the entry of new companies into the market and ensuring fairness with other off-line advertising regulations. However, even where opt-out scheme is adopted, most members have complementary rules that prohibit the delivery of advertising after the recipient has explicitly unsubscribed.

As the opt-in or opt-out schemes have their own advantages and disadvantages, members have established their spam regulation systems to reflect their different policy environments, including the type of spam email/message sender, content, recipient acceptability, and the existence of policy tools.

Consent of Recipient

Due to the nature of an opt-in scheme, all members adopting an opt-in scheme must obtain prior consent, whereas members adopting an opt-out scheme do not require prior consent. However, if the recipient notifies the sender of the intention to unsubscribe after receiving the email or message, the senders must stop further transmission.

For spam emails, out of the members that responded to our survey, 7 members (Australia, Cook Islands, Republic of Korea, Japan, P.R. China, New Zealand, Viet Nam) have mandatory prior consent for spam email as shown in the table below.

APT Members' regulation on Consent of Recipient (spam emails)

Member	Spam emails
Australia	A person must not send, or cause to be sent, a commercial electronic message that has an Australian link; and is not a designated commercial electronic message. However, a person can send, or cause to be sent, a commercial electronic message if the relevant electronic account holder consented to the sending of the message.
Cook Islands	A person must not send, or cause to be sent, a commercial electronic message that has a Cook Islands link without the consent of the relevant electronic account-holder. - unsolicited commercial electronic message means a commercial electronic message that the recipient has not consented to receiving.
Republic of Korea	Where an addressee expresses his or her intention to refuse to receive information or revokes his or her prior consent, no person who intends to transmit advertising information for profit by using an electronic transmission medium shall transmit advertising information for profit.
Japan	A sender shall not send any Specified Electronic Mail to any persons other than the following persons: (i) A person who has notified the sender or the consignor of transmission (referring to a person who consigned transmission of Electronic Mail (limited to an organization for profit and a person in cases where the person is engaged in business); the same shall apply hereinafter) of the request or the consent to send Specified Electronic Mail prior to the transmission thereof
P.R.China	No organization or individual may have the following acts of sending Internet e-mails by itself/himself or upon entrustment: Sending to an Internet e-mail recipient an Internet e-mail containing commercial advertisement contents without the recipient's clear consent;
New Zealand	A person must not send, or cause to be sent, an unsolicited commercial electronic message that has a New Zealand link. - unsolicited commercial electronic message means a commercial electronic message that the recipient has not consented to receiving
Viet Nam	Do not send advertising messages or make advertising calls to the numbers on the Do-Not-Call Register or without prior consents from the users.

For spam message, 7 members adopting the opt-in system (Australia, Cook Islands, Republic

of Korea, Japan, Philippines, New Zealand, Vietnam) have mandatory prior consent for spam messages as shown in the table below.

The Philippines government basically adopts opt-in scheme for spam messages but there is no regulation on spam emails. The National Telecommunications Commission (NTC) regulates broadcast messages by enacting enforcement rules and regulation on broadcasting messaging services in accordance with the Public Telecommunication Services Act. The broadcast messaging Service is a messaging service that allows one to send the same SMS/MMS messages to multiple mobile phones.

APT Members' Regulation on Consent of Recipient (Spam Messages)

Member	Spam messages
Australia	A person must not send, or cause to be sent, a commercial electronic message that has an Australian link; and is not a designated commercial electronic message. However, a person can send, or cause to be sent, a commercial electronic message if the relevant electronic account holder consented to the sending of the message.
Cook Islands	A person must not send, or cause to be sent, a commercial electronic message that has a Cook Islands link without the consent of the relevant electronic account-holder. - unsolicited commercial electronic message means a commercial electronic message that the recipient has not consented to receiving.
Republic of Korea	Where an addressee expresses his or her intention to refuse to receive information or revokes his or her prior consent, no person who intends to transmit advertising information for profit by using an electronic transmission medium shall transmit advertising information for profit.
Japan	A sender shall not send any Specified Electronic Mail to any persons other than the following persons: (i) A person who has notified the sender or the consignor of transmission (referring to a person who consigned transmission of Electronic Mail (limited to an organization for profit and a person in cases where the person is engaged in business); the same shall apply hereinafter) of the request or the consent to send Specified Electronic Mail prior to the transmission thereof
Philippines	Commercial and promotional advertisements, surveys, and other Broadcast/Push messages shall be sent only to subscribers who have prior consent or have specifically opted-in to receive messages.

New Zealand	A person must not send, or cause to be sent, an unsolicited commercial electronic message that has a New Zealand link. - unsolicited commercial electronic message means a commercial electronic message that the recipient has not consented to receiving
Viet Nam	Do not send advertising messages or make advertising calls to the numbers on the Do-Not-Call Register or without prior consents from the users.

Sender Information

Regardless of opt-in or opt-out scheme, the survey found that members with anti-spam policies had common elements: providing sender information and an unsubscribe facility. According to the anti-spam legislation, the senders were required to provide information about their accurate information such as name, email address, and phone number, and to provide an unsubscribe faculty through email or phone number. The unsubscribe facility allows the recipient to indicate that they do not receive messages from the sender and requires the sender to provide accurate contact information.

According to our survey, 9 members (Australia, Republic of Korea, Japan, Singapore, P.R. China, Cook Islands, New Zealand, Hong Kong, Viet Nam) replied that they have email sender information provisions in their anti-spam laws. there are some differences in the type of information provided, but it is basically required to provide accurate return e-mail information, and in some cases to provide the sender's name, address, and phone number.

The Spam Act of Australia states that "a person must not send, or cause to be sent, a commercial electronic message that has an Australian link unless the message clearly and accurately identifies the individual or organization who authorized the sending of the message and the message includes accurate information about how the recipient can readily contact that individual or organization and that information complies with the condition of conditions (if any) specified in the regulation and that information is reasonably likely to be valid for at least 30 days after the message is sent.

Viet Nam has more detailed rules for advertising email requirement. According to the rules, every advertising email shall contain information about the advertisers which shall include the advertiser's name, phone number, email address, geographical address, website/web portal, social network (if any) and shall be clearly displayed and placed right before the unsubscribing option.

APT Members' Regulation on Consent of Recipient (Spam emails)

Member	Information provided
Australia	The identity and contact method of the person (individual/organization) who approved sending the message
Republic of Korea	Sender's name and contact details (e-mail address, phone number, address)
Japan	Personal name or legal name of the said sender, Electronic Mail Address
Singapore	an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted
P.R.China	E-mail envelope information
Cook Islands	The identity of the individual or organization who authorised the sending of the message, accurate information about how the recipient can readily contact that individual or organization
New Zealand	The identity of the person who authorized the sending of the message, accurate information about how the recipient can readily contact that person
Hong Kong	clear and accurate information identifying the individual or organization, clear and accurate information about how the recipient can readily contact that individual or organization
Viet Nam	advertiser's name, phone number, email address, geographical address, website/web portal, social network (if any)

For spam messages, this is similar to the requirement to send sender information in the case of email spam. By enforcing the sending of accurate information, recipients can easily contact the sender.

In the case of Philippines, the National Telecommunications Commission regulates broadcast messages by enacting enforcement rules and regulations on broadcast messaging services in accordance with the Public Telecommunication Services Act. The rules create an opt-in scheme for receiving unsolicited commercial messages sent by SMS or MMS. All such messages must identify the sender and provide sender contact details.

APT Members' Regulation on Consent of Recipient (Spam messages)

Member	Information provided
Australia	The identity and contact method of the person (individual/organization) who approved sending the message

Cook Islands	The identity of the individual or organization who authorised the sending of the message, accurate information about how the recipient can readily contact that individual or organization
Republic of Korea	Sender's name and contact details (e-mail address, phone number, address)
Japan	Personal name or legal name of the said sender, Electronic Mail Address
Singapore	an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted
Philippines	All broadcast messages shall display the name of the PTE. In the case of Content Provider initiated messages, the Content Providers shall indicate their company names or assigned codes. PTEs and content providers shall provide an easy-to-remember hotline number, that may be accessed by voice calls or SMS and free of charge, to assist subscribers who may have queries on subscribed services and/or who wish to opt-out from a particular service or to be excluded from receiving any broadcast messages.
New Zealand	The identity of the person who authorized the sending of the message, accurate information about how the recipient can readily contact that person
Hong Kong	clear and accurate information identifying the individual or organization, clear and accurate information about how the recipient can readily contact that individual or organization
Viet Nam	advertiser's name, phone number, email address, geographical address, website/web portal, social network (if any)

Unsubscribe Facility

An unsubscribe facility allows the recipient to easily indicate their intentions by providing an easy way to unsubscribe. There may also be penalties if senders do not provide such a feature, do not provide a valid return address and postal address, or do not stop sending messages within the time period required by the anti-spam law.

The 9 members with comprehensive spam control frameworks, whether opt-in or opt-out, have in common that the sender provides the recipient with the unsubscribe facility. This often involves providing an email address by default, but sometimes does not specify a particular means of the unsubscribe facility.

As shown in the table below, Australia and Japan explicitly require an electronic address, while Singapore, P.R. China, Republic of Korea, and Hong Kong require sender to provide a other means including email address. Cook Islands, New Zealand, and Vietnam are more inclusive by defining functional unsubscribe facility.

APT Members' Unsubscribe Facility (Spam emails)

Member	Unsubscribe facility
Australia	electronic address
Republic of Korea	Matters regarding measures and methods by which an addressee can readily express his or her intention
Japan	Electronic Mail Address
Singapore	an electronic mail address, an Internet location address, a telephone number, a facsimile number, or a postal address
P.R.China	the means of contact for refusing to continue receiving the said e-mails, including the sender's e-mail address
Cook Islands	functional unsubscribe facility
New Zealand	functional unsubscribe facility
Hong Kong	electronic address or other electronic means
Viet Nam	option to unsubscribe

For the spam messages, 9 members with comprehensive spam control systems, whether opt-in or opt-out, have in common that the sender provides the recipient with an unsubscribe facility. There are many cases where the unsubscribe facility is essentially an electronic address or telephone number, but there are also cases where no specific means is specified.

APT Members' Unsubscribe Facility (Spam messages)

Member	Unsubscribe facility
Australia	electronic address
Cook Islands	functional unsubscribe facility
Republic of Korea	Matters regarding measures and methods by which an addressee can readily express his or her intention
Japan	Electronic Mail Address
Singapore	an electronic mail address, an Internet location address, a telephone number, a facsimile number or a postal address
Philippines	PTEs and content providers shall provide an easy-to-remember hotline number, that may be accessed by voice calls or SMS and free of charge, to assist subscribers who may have queries on subscribed services and/or who wish to opt-out from a particular service or to be excluded from receiving any broadcast messages.

	PTEs and content providers shall also provide methods for subscribers who have opted-in to opt out at some later date. Regular opt-out instructions will be sent once a week for daily subscriptions, once a month for weekly subscriptions. PTEs and Content Providers shall include valid addresses or numbers to which recipients can send requests to cease broadcast messages. They shall also provide command/message on how to opt-out.
New Zealand	functional unsubscribe facility
Hong Kong	electronic address or other electronic means
Viet Nam	option to unsubscribe

Labeling Obligation

Labeling is a necessary policy for clearly identifying and informing users of content suspected of being spam emails or messages and an important factor in helping users identify spam and take necessary actions. Labeling involves adding specific tags or identifiers to subject lines or headers such as “ADV” or “AD” (advertisement) to provide recipients with information about the content of the message. These labels help recipients quickly understand the nature of the message and make informed decisions about whether to open, read, or act on it.

6 members(Republic of Korea, Japan, Singapore, P.R. China, Hong Kong, Vietnam) with comprehensive anti-spam legislation have labeling obligations, which serve as an important regulatory measure to empower users and mitigate the impact of spam. It makes it easier for users to identify and distinguish between legitimate messages and spam and impose minimal burdens on senders while providing significant benefits to users.

Furthermore, the applicability of labeling obligations within anti-spam legislation should be also assessed in the context of each country's unique circumstances and regulatory environment. Factors such as technological infrastructure, legal frameworks, cultural norms, and economic considerations can affect the feasibility and effectiveness of implementing labeling requirements. A tailored approach that takes into account these different factors is therefore essential to ensure the relevance and effectiveness of anti-spam measures on a national scale.

APT Members' Labeling obligation (Spam emails)

Member	Labeling obligation
Republic of Korea	"(Advertising)" must be indicated at the beginning of the title or advertisement information.
Japan	Any sender shall, as specified in the applicable MIC ordinance, upon transmission of Specified Electronic Mails, make such a Specified Electronic Mail correctly display the matters listed as follows on the screen of a communications terminal being used by a person who receives the said Specified Electronic Mail: (i) Personal name or legal name of the said sender (in the cases where there exists a consignor of transmission for the transmission of the said Electronic Mail, the said sender or the said consignor of transmission whoever is responsible for the said transmission) (ii) The Electronic Mail Address for receiving the notification, or codes, including characters, numerical characters and marks, as specified in the applicable MIC ordinance, for identifying telecommunications facilities (iii) Other matters specified in the applicable MIC ordinance.
Singapore	Every unsolicited commercial electronic message shall contain (a) where there is a subject field, a title in the subject field and that title is not false or misleading as to the content of the message; (b) the letters "<ADV>" with a space before the title in the subject field, or if there is no subject field, in the words first appearing in the message to clearly identify that the message is an advertisement; (c) header information that is not false or misleading; (d) an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted.
P.R.China	No organization or individual may have the following acts of sending Internet e-mails by itself/himself or upon entrustment: Failing to indicate the typeface of "advertisement" or "AD" at the former part of the Internet e-mail title information when sending Internet e-mails containing commercial advertisement contents.
Hong Kong	A person shall not send a commercial electronic mail message that has a Hong Kong link if the subject heading of the message, if any, would be likely to mislead the recipient about a material fact regarding the content or subject matter of the message. Commercial electronic messages must not be sent with calling line identification information concealed
Viet Nam	1. The email title shall match the email content and the advertisement therein shall be conformable with advertising laws. 2. Advertising emails shall be tagged. - The tag shall be placed at the beginning of the email title and the tag shall be [QC] or [AD].

	3. Every advertising email shall contain information about the advertisers. - Information about the advertiser shall include the advertiser's name, phone number, email address, geographical address, website/web portal, social network (if any). - Information about the advertiser shall be clearly displayed and placed right before the unsubscribing option. 4. Advertisements of charged services shall specify the charges.

For the spam messages, 5 members with comprehensive anti-spam legislation (Republic of Korea, Japan, Singapore, Hong Kong, Vietnam) have labeling obligations.

APT Members' Labeling obligation (Spam messages)

Member	Labeling obligation
Republic of Korea	"(Advertising)" must be indicated at the beginning of the title or advertisement information.
Japan	Any sender shall, as specified in the applicable MIC ordinance, upon transmission of Specified Electronic Mails, make such a Specified Electronic Mail correctly display the matters listed as follows on the screen of a communications terminal being used by a person who receives the said Specified Electronic Mail: (i) Personal name or legal name of the said sender (in the cases where there exists a consignor of transmission for the transmission of the said Electronic Mail, the said sender or the said consignor of transmission whoever is responsible for the said transmission) (ii) The Electronic Mail Address for receiving the notification, or codes, including characters, numerical characters and marks, as specified in the applicable MIC ordinance, for identifying telecommunications facilities (iii) Other matters specified in the applicable MIC ordinance.
Singapore	Every unsolicited commercial electronic message shall contain (a) where there is a subject field, a title in the subject field and that title is not false or misleading as to the content of the message; (b) the letters "<ADV>" with a space before the title in the subject field, or if there is no subject field, in the words first appearing in the message to clearly identify that the message is an advertisement; (c) header information that is not false or misleading; (d) an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted.
Hong Kong	A person shall not send a commercial electronic mail message that has a Hong Kong link if the subject heading of the message, if any, would be likely to mislead the recipient about a material fact regarding the content or

	subject matter of the message. Commercial electronic messages must not be sent with calling line identification information concealed
Viet Nam	1.Advertising messages shall be tagged. - The tag shall be placed at the beginning of the message, and the tag shall be [QC] or [AD]. 2.Advertisements of charged services shall specify the charges.

Regulation on address harvesting software

One of the main focuses of comprehensive anti-spam legislation is the regulation of address harvesting software. Address harvesting software is a powerful tool in the spammers' arsenal, facilitating the rapid collection and use of large volumes of email addresses. Therefore, its regulation is considered essential to mitigate the widespread nuisance and potential harm caused by spam. By limiting the effectiveness of address harvesting software, the authorities aim to reduce the volume and impact of unsolicited email, thereby improving user experience and safeguarding the online environment.

According to our survey, 8 members with comprehensive anti-spam laws regulate address harvesting software. Since address harvesting software maximises the damage of spam by making it easy for spammers to send large volumes of e-mail to recipients, regulation is desirable and can be effective for user convenience. However, whether or not address harvesting software is regulated, the need to do so should be considered in the light of the different situations and environments in each member.

APT Members' Regulation on address harvesting SW

Member	Regulation on address harvesting software
Australia	Address-harvesting software and harvested-address lists must not be supplied, acquired, used
Republic of Korea	No person who transmits advertising information for profit by using an electronic transmission medium shall take any of the following measures: Measures to automatically generate an addressee's contact information, such as telephone numbers and e-mail addresses, by combining figures, codes, or letters; Measures to automatically register telephone numbers or e-mail addresses for the purpose of transmitting advertising information for profit;
Japan	(Prohibition of Transmission Using Fictitious Electronic Mail Address) No sender shall send Electronic Mails to Fictitious Electronic Mail Addresses for the purpose of sending many Electronic Mails for their own or other's sales

	activities.
Singapore	(Use of dictionary attack and address harvesting software) This shall apply to all electronic messages, whether or not they are unsolicited commercial electronic messages. No person shall send, cause to be sent, or authorize the sending of an electronic message to electronic addresses generated or obtained through the use of (a) a dictionary attack or (b) address harvesting software.
P.R.China	No organization or individual may have the following acts: Using the Internet e-mail addresses of others, which are got by online automatic collection, by arbitrary alphabetical or digital combination or by other means, in selling, sharing or exchanging Internet e-mails, or in sending Internet e-mails to the e-mail addresses got by the foregoing means.
Cook Islands	A person must not supply or offer to supply address-harvesting software; or a right to use address-harvesting software; or a harvested-address list; or a right to use a harvested-address list. A person must not acquire address-harvesting software; or a right to use address-harvesting software; or a harvested-address list; or a right to use a harvested-address list. A person must not use address-harvesting software; or a harvested-address list, If the person is an individual who is physically present in the Cook Islands at the time of the use; or a body corporate or partnership that carries on business or activities in the Cook Islands at the time of the use.
New Zealand	A person must not use address-harvesting software or a harvested-address list in connection with, or with the intention of, sending unsolicited commercial electronic message.
Hong Kong	(Supply of address-harvesting software or harvested-address list) No person shall supply or offer to supply (a)address-harvesting software; (b)a right to use address-harvesting software; (c)a harvested-address list; or (d)a right to use a harvested-address list, to another person (the customer) for use in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent. A person who knowingly contravenes commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years. (Acquisition of address-harvesting software or harvested-address list) No person shall acquire (a)address-harvesting software; (b)a right to use address-harvesting software; (c)a harvested-address list; or (d)a right to use a harvested-address list, for use in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are

	sent. A person who knowingly contravenes commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years. (Use of address-harvesting software or harvested-address list) No person shall use (a)address-harvesting software; or (b)a harvested-address list, in connection with, or to facilitate, the sending of commercial electronic messages that have a Hong Kong link without the consent of the registered users of the electronic addresses to which they are sent. A person who knowingly contravenes commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years. (Sending of commercial electronic message to electronic address obtained using automated means) No person shall send a commercial electronic message that has a Hong Kong link to an electronic address that was obtained using an automated means. A person who knowingly contravenes commits an offence and is liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years. automated means mean an automated process that generates possible electronic addresses by combining letters, characters, numbers or symbols into numerous permutations;

Bulk requirement

Bulk spam emails and messages regulation refers to the regulation of sending emails or messages in bulk and is generally implemented to mitigate the inconvenience and damage caused to users by spam and to protect their privacy.

Most members don't have regulations for bulk requirement, but we found that Singapore has detailed regulations for this. Unlike other members, Singapore regulates spam only if it meets the requirement for sending emails in bulk.

Singapore regulates the bulk requirement in the Spam Control Act as below:

> Any person who sends, causes to be sent or authorises the sending of unsolicited commercial electronic messages in bulk shall comply with the requirements below.
>
> Electronic messages shall be deemed to be sent in bulk if a person sends, causes to be sent or authorizes the sending of –
>
> (a) more than 100 electronic messages containing the same or similar -matter during a

24-hour period;

(b) more than 1,000 electronic messages containing the same or similar -matter during a 30-day period;

(c) more than 10,000 electronic messages containing the same or similar -matter during a one-year period;

2.4. Penalties

Most members with anti-spam legislation provide for sanctions for violations of relevant legal provisions. In most members, when a sender violates the law, the first step is for the relevant Ministy to issue an administrative order to correct the violation, followed by a fine or imprisonment by the Ministry or the court.

In particular, some members have different levels of fines depending on the content of the spam, such as South Korea. Korea has different penalty standards, i.e., the degree of penalty is differentiated by the contents type of spam, e.g., fine for financial product advertisement spam vs. imprisonment for gambling advertisement spam) depending on the type of advertisement.

In other cases, fines vary depending on which provision of the law has been violated, with the strongest penalties in Vietnam ranging from VND 80m to VND100m for sending advertising messages to 'Do-Not-Call' recipients, while fines range from VND 5m to VND 10m for violating clear prior consent.

APT Members' Penalty Provisions

Members	Penalties
Australia	Fine for the individuals up to AUD 84,000 per day (first offense) The penalties vary depending on the legislative provision, the number of breaches, who is charged the penalty(ACMA or courts)
Cook Islands	Pecuniary penalty for the individuals up to $ 200,000, for the corporation $1,000,000
Republic of Korea	Fine not exceeding KRW 1,000,000 or imprisonment with labor for up to 1 year
Japan	Fine up to JPY 1,000,000 or imprisonment for up to 1 year
Singapore	Statutory damage not exceeding SGD 25 for each message, the maximum not exceeding SGD 1 million without proving the actual loss
P.R. China	Fines up to CNY 10,000 (This can increase to CNY 30,000, depending on the illegal income from the violations)

New Zealand	Pecuniary penalty for the individuals not exceeding NZD 200,000, for the organisation NZD 500,000
Hong Kong	Fines up to HKD 500,000 in addition to a daily fine up to HKD 1,000 per day for the duration of the violation
Philippines	Fines depending upon the violation provision and numbers
Vietnam	Fines depending upon the violation provision

3. Non-Regulatory Approaches

Regulatory approaches can be enforced and lead to the punishment of illegal spammers, but they are not sufficiently effective in reducing the volume of spam or changing user behaviour in a proactive manner. Therefore, a multi-dimensional approach should be considered to maximise the effectiveness of spam regulation, including technical methods by telcos, self-regulation, education/campaigns to raise user awareness, and international cooperation. For this purpose, the establishment of a public-private partnership system can promote the development of the digital economy by increasing the reliability of communication services.

3.1 Technical measures

Internet Service Providers, other network operators, and telcos continue to develop and important role in reducing the amount of spam in users' inboxes, but other technology solutions should be complementary and overlapping to maximise their effectiveness.

Of the members who responded to the survey, 10 members (Australia, Cambodia, Republic of Korea, Thailand, Brunei, Micronesia, Lao PDR, Pakistan, Singapore, Sri Lanka) explicitly responded the technical measures by telecommunication service providers.

Republic of Korea takes government-led technological measures. The Information and Communications Network Act stipulates that the government may develop and distribute software to block spam. Accordingly, the government (Korea Communication Commission) and KISA(Korea Information & Security Agency) actually prepared RBL (Realtime Blocking List), MRBL (Mobile Realtime Blocking List), White domain (a kind of whitelist), and SPF (Sender Policy Framework) and provide them to Internet Service Providers and telcos.

In Singapore, telecommunication service providers, are required to implement anti-spam measures such as blocking scam SMS/calls.

In Thailand, an Internet Service Provider (True Internet) provides a technical solution called ‘Mailed Cleaner’ which filters and scans all incoming emails to prevent spam and any virus. Once detected, the system eliminates them before sending the mails to the user’s mail server.

Member	Technical measures
Australia	Spam filtering by telecommunication/ internet service providers
Cambodia	MaxBIT spam filter
Republic of Korea	KCC and KISA develop and distribute software to block spam. KISA-RBL, KISA-MRBL, White domain, SPF
Singapore	blocking scam SMS/calls
Lao PDR	SMS inspection system
Thailand	Mail cleaner service by internet service provider
Pakistan	Anti-spam filters
Brunei	Technical measures by network operator
Micronesia (Federated States of)	Technical measures by Telecon Corporation
Sri Lanka	Technical measures by each organization

3.2. Self-Regulation & Education and Awareness raising

The promotion of self-regulation by service providers and education and awareness-raising activities for users are indirect and complementary unlike direct government regulation. While direct regulation by the government has a strong effect by imposing enforcement and penalties for violations, it is insufficient to elicit voluntary and proactive efforts from service providers. Therefore, it is increasingly important for the government to promote self-regulation of service providers through incentives, while educating users on how to respond to spam emails/messages and raising awareness through campaigns.

In terms of self-regulation, we found that Republic of Korea, New Zealand, Hong Kong, Thailand, and Singapore operate self-regulatory schemes. Republic of Korea publishes a spam distribution status report (semi-annually) and regularly publishes the spam distribution volume of each telecommunication service provider to enhance the voluntary spam mitigation efforts. To this end, an indicator has been established to compare the spam reduction efforts of each service provider.

Singapore, New Zealand, Thailand, and Hong Kong have created Spam control Guideline or Codes of Practice to promote voluntary spam reduction efforts by service providers.

In Australia, as described earlier, a study was conducted into the introduction of government-level self-regulation, which concluded that direct government regulation was more appropriate than self-regulation given the conditions, including the level of co-operation among service providers in Australia, and international examples. Most Members, as well as Australia, were found to rely more on direct regulation than self-regulatory schemes.

In terms of the education and Awareness raising activities, 11 members (Australia, Republic of Korea, P.R. China, Indonesia, Pakistan, Papua New Guinea, Singapore, Malaysia, Hong Kong, Brunei, Sri Lanka) that responded to the survey have government-level education and awareness activities. Most of them are conducting a combination of education for operators and education for users, and they are raising awareness through various methods such as creating and distributing educational materials and holding seminars.

Member	Self-regulation	Education/ Awareness raising
Australia	No / The direct regulatory model remains appropriate.	ACMA provides education to both industry and consumers
Cambodia	No	No
Cook Islands	No	N/A
Republic of Korea	Spam distribution status report (half yearly)	For business operators; business briefing sessions and educational content production/ For users; production of educational materials and educational contents
Japan	N/A	N/A
Singapore	Spam control guidelines/ Code of practice by industry association	Public education
P.R.China	N/A	Education/awareness raising
Lao PDR	No	No
Malaysia	N/A	Education/awareness raising
Nepal	No	No
New Zealand	Code of practice by private associations	N/A
Hong Kong	Code of practice by private associations	education and publicity programmes to educate the public; public seminars, roving exhibitions
India	N/A	N/A
Indonesia	No	Education and awareness raising policy
Thailand	Code of Practice	no
Pakistan	No	Public awareness messages, Advertisement
Papua New Guinea	No	Awareness raising through media
Philippines	N/A	N/A
Viet Nam	N/A	N/A
Bhutan	No	No

Member	Self-regulation	Education/ Awareness raising
Brunei	No	general online safety awareness program: online safety learning materials, publish videos, audios and awareness materials for broadcast, awareness talks
Micronesia (Federated States of)	No	No
Kiribati	No	No
Sri Lanka	No	Education and awareness through social media, sending SMS to subscribers by operators
Tonga	No	No

3.3. International Cooperation

The adverse effects of the development and spread of the Internet and telecommunications, including spam, inevitably transcend national borders. Therefore, there is a general consensus among members in the Asia-Pacific region on the need for international cooperation to combat spam. However, only a few members are actively participating in international cooperation initiatives, and further engagement should be encouraged.

A prime example of an international cooperation initiative in which members are involved is UCENet. The initiative, which began with the London Action Plan and has been maintained for over 15 years, includes 6 members (Australia, Republic of Korea, Japan, P.R. China, Malaysia,Hong Kong). In 2018, Republic of Korea has established UCENet's regional initiative, UCENet Asia-Pacific, to further enhance cooperation in the region.

More recently, 13 members (Australia, Republic of Korea, Japan, Singapore, P.R. China, Lao PDR, Malaysia, New Zealand, Indonesia, Thailand, the Philippines, Viet Nam, Brunei) have signed the RCEP (Regional Comprehensive Economic Partnership) Agreement, which will strengthen cooperation in the region and facilitate national spam-fighting efforts.

UCENet	UCENet Asia-Pacific	RCEP agreement
Australia, Republic of Korea, Japan, P.R. China, Malaysia, Hong Kong	Australia, Republic of Korea, Japan, New Zealand	Australia, Republic of Korea, Japan, Singapore, P.R. China, Lao PDR, Malaysia, New Zealand, Indonesia, Thailand, Philippines, Viet Nam, Brunei

In addition, we found that each member is strengthening cooperation with other regional partnerships and countries to counter spam.

Australia is a signatory to several free trade agreements in force which include commitments to address spam, including The Comprehensive and Progressive Agreement for Trans-Pacific Partnership and the Peru-Australia Free Trade Agreement. Moreover the ACMA, Australia's regulatory authority also has MoUs with both the USA and Canada which specifically address information sharing and collaboration on spam issues.

Republic of Korea has participated in the GSMA spam reporting service which is a project to build a global reporting system that collects mobile spam data from around the world and analyzes major statistics and trends.

4. Key Features

Legislation

According to OECD Anti-Spam Toolkit of recommended Policies and Measures (2006), to enhance the effectiveness of spam response, it stresses the need to establish a coherent and harmonised spam response framework, and in particular the enactment of anti-spam legislation at a fundamental level to clearly define what is and is not permitted. In parallel, the enforcement and implementation of the legislation is also crucial, as are timely and prompt enforcement actions and penalties for violations. Furthermore, this regulatory framework needs to be combined and enforced with private sector initiatives, including the continuous development and promotion of technological solutions

The anti-spam laws in the Asia-Pacific region evolved according to the circumstances and environment of each country, as the applicable to each country must be designed in consideration of the legal, economic, and social factors of each country, and the intensity of regulation should also be considered in accordance with the level of development of the Internet/telecommunications. However, spam control and response are essential in that it ensures the stability of the network and provides the basis for the launch of various new user-friendly services.

As we have seen above, only 9 members of 16 that responded to the survey, have anti-spam laws. Therefore, there is a significant need to support the ongoing development of legal frameworks in those members that do not have laws, and to continue to provide updates on spam-related developments in the Asia-Pacific region to enhance the fight against spam.

Adoption of Main Elements

Most anti-spam laws of the Members have opt-in/opt-out schemes, sender information, consent of recipient, and labelling obligation as provisions. The opt-in/out schemes and sender information play an important role in reducing spam emails/messages and protecting recipients' privacy. They are also crucial for tracking senders and distinguishing trusted senders.

Clearly indicating in the subject line of an email or text that it is an advertisement allows recipients to know in advance what the email is about and helps filter out spam. Additionally, some countries regulate the use of address harvesting software or automatically compiled address lists, with the goal of protecting privacy and preventing the further spread of spam.

However, the level of these regulations should be determined by each member's decision to effectively combat spam according to the policy environment. In particular, depending on the stage of evolution of ICT technology, overregulation could delay or even hinder the development of technological advancements and services, thus the appropriate harmonisation of the ICT environment and the level of regulation could be one of the most important considerations for policy makers.

Differential penalty levels

Members' anti-spam laws also stipulate penalties for violations of the law. Overall, these penalties aim to discourage spamming and promote responsible communication practices. Typical penalties for violating anti-spam laws include fines, injunctions, and civil lawsuits. The level of sanctions varies depending on the number of violations, the type of violation, or the contents type of spam email/message.

Repeat offenders may face harsher penalties than first-time violators. Some members' laws impose escalating fines or other sanctions for each subsequent violation. The severity of the violation can influence the penalties. For instance, intentionally deceptive practices or targeting vulnerable groups might result in more severe consequences. Different types of spam may be subject to different penalties. For example, the sending of purely advertising information and the sending of advertising information for profit are sanctioned at different levels.

Weak Self-regulation

In order to respond promptly to the evolving technologies driven by rapid technological changes, it is essential to have self-regulation by stakeholders, as legal regulations alone have limitations. Nonetheless, it has been observed that self-regulation is not actively implemented in many members. To overcome the rigidity of legal regulations and flexibly respond to rapidly changing technological advancements, private sector efforts are necessary. This underscores the growing need for self-regulation in the Asia-Pacific region.

5. Activities of APT

5.1. Research Reports

We have been compiling the results of the surveys and trends in international collaboration over the past two years and have made them available to the Members in the research reports. This allows the Members to understand the current status of policies that have been established according to the environment of each member, and to identify the advantages and disadvantages of policies through comparative analysis.

The research also needs to be improved in the future, given the limitations of the desk study, which currently relies primarily on surveys and therefore lacks analysis of non-participating Members.

5.2. APT Web Dialogue

The APT Web Dialogue is aimed to facilitate discussion and sharing of information, knowledge and experiences among the Members as well as to provide an opportunity for coordination on issues if necessary.

We conducted the survey to identify the current state of spam response in the region, also organized the APT Web Dialogue in both 2021 and 2022, aiming to furnish policymakers in the Asia-Pacific region with crucial insights into spam management and facilitate discussions on leveraging cutting-edge technologies for efficient spam mitigation.

In 2021, we sought to address the worldwide shifts and approaches regarding unsolicited commercial communications, a critical concern in the digital era due to its potential to undermine the credibility of communication platforms, apps, and services, as well as erode the trust of online users. Dr. Archana G. Gulati from the Department of the Telecommunications, India introduced the current situation, trends and share her insights on the issue and discussed future strategies and possible response with online participants.

In 2022, we shared the result of the research on the current status of unsolicited commercial messages policies and regulations of the Members through the surveys and outlined the legislation, legal and technical measures, self-regulation, and awareness-raising activities of the 17 countries that responded to our survey.

In addition, expert panelists, Mr. Francis Zhang, from the Personal Data Protection Commission, Singapore and Mr. Kyeongsik Park from the Korea Internet Security Agency, Ms. Susan Park from Bae Kim & Lee LLC, Korea Ms. Kathleen Silleri from the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Australia, discussed how to effectively address to evolving spamming technologies in response to rapidly

changing technology trends.

< APT Web Dialogues for the Unsolicited Commercial Messages >

6. Way Forward

The three-year spam policy survey provided a broad overview and thorough understanding of the current state of spam response at each of our member organisations. This comprehensive survey, which aimed to capture the state of spam policy where it had not been done before, scrutinised the effectiveness and scope of various policies, highlighting strengths and weaknesses in each member's strategy. In addition to this broad overview, the survey also included a comparative analysis of the spam policies of several of our members. Based on the results of the survey, which was completed by 25 members in total, we expect this comparative study to play an important role in identifying best practices and laying the groundwork for an informed discussion on how to increase the effectiveness of spam response mechanisms.

However, there are important trends that have not yet been identified and we expect that future research will be able to provide more detailed and granular information by delving deeper into the nuances of anti-spam strategies. In particular, future research will look more closely at non-regulatory approaches, such as technical measures, self-regulation and awareness raising efforts by individual members, which were not covered in detail in our survey. As technology evolves, new types of spam continue to emerge and threats to a secure ICT environment

continue to grow, including large volumes of email not filtered out by regulatory approaches and new fraudulent schemes disguised as gambling, stocks and more. Our efforts to explore multi-pronged approaches will therefore play an important role in developing an effective global response to the ever-evolving spam problem, while identifying more specific and actionable measure.

Annex 1. APT Letters(2021-2023)

ASIA-PACIFIC TELECOMMUNITY
12/49 Soi 5, Chaeng Watthana Road, Bangkok 10210, Thailand

Ref. APT/2021/EBC-K(KISA)-02 20 August 2021

Dear Sir/Madam,

Subject: APT Research Project on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia-Pacific Region"

I am pleased to inform you that the Asia-Pacific Telecommunity (APT) is conducting a research on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia-Pacific Region", which was approved at the 44th Session of the Management Committee of the APT (MC-44) in 2020 and is supported by the Extra-Budgetary Contribution from the Republic of Korea. This research intends to facilitate sharing of information and best practices among APT members regarding policies and legislations on issues related to spam, particularly given the increasing threats from the unsolicited, unwanted and harmful spam and the need to find appropriate way to cooperate among APT Members.

As an important part of the research, I would like to request your Administration to kindly cooperate to this research by filling in the questionnaire (https://forms.gle/R2z9pEesvvNaDGc3A) which is designed to gain a better idea of anti-spam framework in APT member countries, including issues they are facing, relevant policies/legislations, and international cooperation, etc. It would take around 20 minutes to complete this online survey. Please be assured that the information provided through this questionnaire will be used solely for the research purpose.

To ensure timely arrangement, I would be grateful if your Administration would fill in the questionnaire which is provided by the above Google Form link **by 30 September 2021**. For further information or assistance, please contact APT Secretariat by email to aptresearch-privacy@apt.int or by fax: +66 2 573 7479.

I thank you in advance for your cooperation and look forward to your early response.

Yours sincerely,

M. Kondo

ASIA-PACIFIC TELECOMMUNITY
12/49 Soi 5, Chaeng Watthana Road, Bangkok 10210, Thailand

Ref. APT/KISA-KOR/2022-02 15 September 2022

Dear Sir/Madam,

Subject: APT Research Project on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia-Pacific Region"

I am pleased to inform you that the Asia-Pacific Telecommunity (APT) is conducting a research project on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia-Pacific Region", which was approved at the 45th Session of the Management Committee of the APT (MC-45) in 2021. This project is supported by the Extra Budgetary Contributions from the Republic of Korea. This research intends to facilitate sharing of information and best practices among APT Members and Associate Members regarding policies and legislations on issues related to spam, particularly given the increasing threats from the unsolicited, unwanted and harmful spam and the need to find appropriate way to cooperate among APT Members.

As an important part of the research, I would like to request your Administration to kindly cooperate with this research by filling in the online questionnaire (https://forms.gle/H4N6gSM6jpm8N3Mz5) which is designed to collect information about anti-spam framework in APT Member administrations, including issues they are facing, relevant policies/legislations, and international cooperation, etc. It takes around 20 minutes to complete this survey. Please be assured that the information provided through this questionnaire will be used solely for the research purposes.

To ensure timely arrangement, I would be grateful if your Administration would fill in the questionnaire which is provided by the above Google Form link **by 15 October 2022**. For further information or assistance, please contact the APT secretariat by email aptresearch-privacy@apt.int or by fax: +66 2 573 7479.

I thank you in advance for your cooperation and look forward to your early response.

Yours sincerely,

M. Kondo

Masanori Kondo
Secretary General

ASIA-PACIFIC TELECOMMUNITY
12/49 Soi 5, Chaeng Watthana Road, Bangkok 10210, Thailand

Ref. APT/KISA-KOR/2023-02 13 October 2023

Dear Sir/Madam,

Subject: APT Research Project on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia-Pacific Region"

I am pleased to inform you that the Asia-Pacific Telecommunity (APT) is conducting a research project on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia-Pacific Region", which was approved at the 46th session of APT Management Committee (MC-46) in 2022 for continued implementation from the previous year. This project is supported by the extra budgetary contributions from the Republic of Korea and is currently in its third year of research. This research intends to facilitate sharing of information and best practices among APT Members and Associate Members regarding policies and legislations on issues related to spam, particularly given the increasing threats from the unsolicited, unwanted, and harmful spam and the need to find appropriate ways to cooperate among APT Members.

As an important part of the research, I would like to request your Administration to kindly cooperate with this research by filling in the online questionnaire (https://forms.gle/kpVsBREmGsEDC3CT9) which is designed to collect information about anti-spam framework in APT Member administrations, including issues they are facing, relevant policies/legislations, and international cooperation, etc. It takes around 20 minutes to complete this survey. Please be assured that the information provided through this questionnaire will be used solely for the research purposes.

To ensure timely arrangement, I would be grateful if your Administration would fill in the questionnaire which is provided by the above Google Form link **by 15 November 2023**. For further information or assistance, please contact the APT secretariat by email aptresearch-privacy@apt.int.

I thank you in advance for your cooperation and look forward to your early response.

Yours sincerely,

M. Kondo

Masanori Kondo
Secretary General

To : Afghanistan, Bangladesh, Democratic People's Republic of Korea, Fiji, Iran, Maldives, Marshall Islands, Mongolia, Myanmar, Nauru, Palau, Samoa, Solomon Islands, Tuvalu, Vanuatu, Macau, Niue

E-mail: apthrd@apt.int, Web Site: www.apt.int, Telephone: + 66 2 5730044, Fax: + 66 2 5737479

Annex 2. APT Survey Questionnaire

Questionnaire for APT research on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages in Asia-Pacific Region"

□ Background

In order for electronic communication platforms, applications and services contribute to economic and social development, they must be reliable, efficient and trustworthy. Today, however, e-mail and other electronic communication tools are largely threatened by unsolicited, unwanted, and harmful electronic commercial messages, commonly known as spam. Spam, which began as electronic messages to advertise commercial products or services, has evolved over the past years, and become to have negative impact, which can be deceptive, cause network disruptions, and form some sorts of fraud that could be used as a stepping stone for spreading viruses and other malware.

Accordingly, there are several researches on unsolicited commercial messages such as the one conducted by ITU and other international collaboration initiatives.

However, in Asia-Pacific region, there is not relevant and updated information on the current status of APT members regarding unsolicited commercial messages sufficiently.

Under such circumstances, the Strategic Plan of the APT for 2021-2023 adopted by the 15th Session of General Assembly of the APT (GA-15) enumerates five strategic pillars and "Trust and Safety" is one of them. The strategic direction of this pillar is "to develop and maintain secure, trusted and resilient telecommunication/ICT networks and services". Accordingly, the 44th and 45th session of the Management Committee (MC-44/MC-45) of the APT in 2020 approved to conduct a research on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia Pacific Region" (MC44/OUT-18, MC45/OUT-09).

In line with these situations, from 2021 to 2023, APT-KISA joint research will focus on not only figuring out the current status of spam related issues, legislation, and policies of our

Members, but also finding collaborative response measures to prevent spam in our region. Through this research, global and regional best practices and policy experiences can be shared among APT Members and facilitate its policy/regulatory formulation as necessary.

In this regard, I would like to request your Administration to kindly cooperate to the research by filling in this questionnaire which is designed to gain a clearer idea of anti-spam framework in your country such as the current situation in each APT Member including issues they are facing, relevant legislations/policies, and international cooperation on this matter, etc. Please be assured that the information provided through this questionnaire will be used solely for the research purpose.

In addition, based on the research result, the APT is preparing to provide capacity building programmes in order to support member countries to strengthen and deepen its legal insights and policy framework. This programme would be online training to APT member countries on request basis to provide information not only on best practices of APT members but also global norm and trend in anti-spam policy/legislation area. Also, APT has a plan to provide consultancy to APT member countries on request basis, as an APT Expert Mission, to help member countries to draft anti-spam laws and policies as required. In this regard, APT Secretariat will circulate invitation letter to ask your needs and requirements for those APT capacity building programmes.

I thank you in advance for your cooperation and look forward to your early response.

Ⅰ. General Information on spam

1. How do you define spam, and is that definition contained in national law or regulation? If it does, please fill in the following information:

1-1. Definition of spam in national law or regulation (Please specify the name of law or regulation):

1-2. If you don't have definition in national law or regulation, is there any other source of definition in your country (for example, in Guidelines, Directives, etc.) If it does, please describe it in detail:

2. How do you identify and measure spam in the operational environment? If available, please provide:

2-1. Types of spam (e.g., e-mail spam, SMS/MMS spam, spam in IP-based application (SNS, instant messenger, bulletin board), voice call spam, etc.)

2-2. Volume of spam traffic, both quantity and as a percentage of all traffic (Monthly and yearly statistics of the previous data for the last three-year period). If your country has a reporting system on spam from citizens, please provide the volume of spam report from citizens (Monthly and yearly statistics of the previous data for the last three-year period)

2-3. The source, routes of spam traffic (If available, please provide picture of routes)

2-4. What are the current challenges related to spam in your country? Please fill in the following information:

1. Existence of issues related to spam: □ 1) Yes □ 2) No

2. Types of issues: □1) legislation □ 2) technical issue □ 3) government-private sector cooperation □ 4) law enforcement □ 5) international cooperation □ 6) others

3. Please describe in detail if your country has any challenges related to spam:

Please present an English URL address or a website address that can give information on the relevant challenges.

3. Do you identify or measure spam by types of contents (e.g., gambling, loan, medicine, financial product, etc.) in the operational environment? If so, please provide:

3-1. Categorized types of spam based on advertisement type (e.g., gambling, loan, medicine, financial product, etc.) in your country

3-2. If your country has different penalty standards (i.e., the degree of penalty is

differentiated by the contents type of spam e.g., fine for financial product advertisement spam vs. imprisonment for gambling advertisement spam) depending on the type of advertisement, please provide the information.

3-3. If the government authority in charge of spam (e.g. Ministry of Communications, Telecommunications Regulatory Authority) cooperates organizations related to the type of advertisement(spam contents) (e.g., illegal loans - Financial Supervisory Authority, medicine- Health Authority, etc.), please provide the activities for cooperation between them.

4. Which entity/stakeholder in your country is/are engaged in anti-spam activities? (Multiple choices)

□ 1) Government

□ 2) Telecommunication Service Providers

□ 3) Industry associations

□ 4) Non-governmental organizations

5. If you have any information on the anti-spam activities that the private sectors (Telecommunication Service Providers, Industry associations, Non-governmental organizations, etc.) are doing currently, please describe it in detail:

6. If you are able to categorize spam by its target (e.g., the population at large, children, elderly people, families, local communities, small businesses, local authorities, etc.), describe the process by which you are able to do so?

7. Have you estimated how much spam incidents cost to the economy of your country or your organization? If so, please provide data for the last three-year period, and describe your methodology for establishing the costs.

8. As mentioned in the background of this questionnaire, the APT is preparing capacity building programs to help member countries to strengthen legal insights and policy framework. Which one do you think you need at your country? (Multiple choices)

□ 1) Training to APT member countries' government officers, etc.

□ 2) Consulting through APT Expert Mission

□ 3) Others: Please specify them

9. If you choose training, what are the most needed training contents? (Multiple choices)
   □ 1) Overall outline for anti-spam legal framework
   □ 2) Global norm and trends
   □ 3) Specific rules and regulations
   □ 4) Analysis on each APT Members' current regulations, problems
   □ 5) Best practices, recent developments, etc.
   □ 6) Interactive workshop for finding solutions
   □ 7) Others: please specify them

10. Who are the most appropriate educational target? (Multiple choices)
   □ 1) Director General level government officers who are in charge of spam related issues
   □ 2) Director level government officers who are in charge of spam related issues
   □ 3) Deputy director level government officers who are in charge of spam related issues
   □ 4) Manager level government officers who are in charge of spam related issues
   □ 5) Researcher in public research agency
   □ 6) Others: please specify them

11. If you choose consulting, what are the most needed help? (Multiple choices)
   □ 1) Interview with domestic experts
   □ 2) Information sharing from the experts dispatched by APT
   □ 3) Drafting new Anti-Spam Act
   □ 4) Drafting amendment to current law
   □ 5) Drafting strategic plan for anti-spam
   □ 6) Others: please specify them

II. Legislation on spam

1. Does your country have general anti-spam act? If it does, please fill in the following information:

   1-1. Existence of general anti-spam act: ☐ 1) Yes ☐ 2) No

1-2. URL:

1-3. Names of Act and date of enactment:

1-4. Name of government authority that handles spam related legal issues

2. If your country doesn't have any general act on spam, does your country have any plan to legislate one? If it does, please fill in the following information:

2-1. Existence of legislation plan: ☐ 1) Yes ☐ 2) No

2-2. preparation stage: ☐1) planning ☐ 2) research ☐ 3) drafting ☐ 4) under public consultation ☐ 5) under legislative review

2-3. expected time of legislation: ☐1) within ten years ☐ 2) 3-5 years ☐ 3) 1-2 years

2-4. If your country has draft legislation, please share it

Please present an English URL address or a website address that can give information on the relevant issues.

3. If your country doesn't have any general act on spam, how does your Administration feel the need to legislate general anti-spam act?

☐ 1) No need

☐ 2) Cannot take a position

☐ 3) a little needed

☐ 4) very needed

4. If you don't have a plan, could you identify the reason?

☐ 1) lack of resources (information, experts, fund, etc.)

☐ 2) never experienced serious spam related issues, so we don't have any need to enact general anti-spam act

☐ 3) other laws such as criminal law, consumer protection law, etc, can cover spam issues, so we don't have any need to enact general anti-spam act

5. If you chose 3) in the previous question 4, please fill in the following information:

5-1. Names of Act and date of enactment:

5-2. URL:

5-3. Name of government authority that handles legal issues

6. Aside from the government authority, is there any organization(s) (for example a market dominant network operator) which has the responsibility for monitoring and countering spam in your country? What are those responsibilities?

7. If there is a national focal point for spam matters, please provide its contact information such as email address.

III. Self-Regulation and Public-Private Partnership

1. Does your country have any anti-spam self-regulation scheme (self regulation mechanism developed and operated by service providers, industry associations, and non-governmental organizations. Self-regulation scheme is not regulated by the government laws or regulations but by self-organized regulation mechanism)? If it does, please fill in the following information:

1-1. Existence of self-regulation scheme: ☐ 1) Yes ☐ 2) No

1-2. If it has a webpage, please provide its' URL:

1-3. Names of self-regulation scheme and date of starting:

1-4. Name of administrative institution (e.g. industry association) that handles related issues

2. If your country doesn't have any anti-spam self-regulation scheme, does your country have any plan to create one? If it does, please fill in the following information:

2-1. Existence of plan: ☐ 1) Yes ☐ 2) No

2-2. preparation stage: □1) planning □ 2) research □ 3) drafting □ 4) under public consultation □ 5) under review before launch

2-3. If your country has draft plan of creating self-regulation scheme and can share it

Please present an English URL address or a website address that can give information on the relevant issues.

3. If you don't have a plan, could you identify the reason? (Multiple choices)

□ 1) lack of resources (information, experts, fund, etc.)

□ 2) never experienced serious spam related issues, so we don't feel any need

□ 3) Others: Please specify them

4. In the private sector, what is the expected or mandated role of the network operator in monitoring and countering spam? What is the relationship between the private sector network operator(s) and the government?

5. What other organizations (e.g., private, non-profit) have the responsibility for countering spam? What are those responsibilities?

IV. Technical solutions

1.Has your country or organizations or service providers in your country implemented technical solutions to counter spam? (e.g., recognition and filtering mechanisms, etc.) If so, please fill in the following information:

1-1. Existence of technical solutions: □ 1) Yes □ 2) No

1-2. If there is a webpage regarding these technical solutions, please provide the URL:

1-3. Names of technical solutions and date of establishment:

1-4. Name of administrative institution that handles related issues

2. If your country didn't implement any technical solutions, does your country have any plan to implement one? If it does, please fill in the following information:

2-1. Existence of plan: □ 1) Yes □ 2) No

2-2. preparation stage: □1) planning □ 2) research □ 3) drafting □ 4) under public consultation □ 5) under review before launch

2-3. If your country has draft plan to implement and can share it

Please present an English URL address or a website address that can give information on the

relevant issues.

3. If you don't have a plan, could you identify the reason? (Multiple choices)

□ 1) lack of resources (information, experts, fund, etc.)

□ 2) never experienced serious spam related issues, so we don't feel any need

□ 3) Others: Please specify them

4. If your country has implemented technical solutions, how is the effectiveness of the solutions measured? If available, please provide data for the last three-year period, and describe your methodology for measuring the effectiveness.

5. Which ITU-T Recommendations or other standards, if any, are used to counter spam (e.g. ITU-T, 3GPP, etc.)?

V. Education and raising awareness

1. Does your country have any anti-spam policy related to the education and awareness-raising on spam? If it does, please fill in the following information:

1-1. Existence of policy: □ 1) Yes □ 2) No

1-2. URL:

1-3. Please provide the lists of activities of education and awareness-raising policy and date of starting:

1-4. Name of administrative institution that handles related issues

2. If your country didn't have any education and awareness-raising policy, does your country have any plan to create one? If it does, please fill in the following information:

2-1. Existence of plan: □ 1) Yes □ 2) No

2-2. preparation stage: □1) planning □ 2) research □ 3) drafting □ 4) under public consultation □ 5) under review before launch

2-3. If your country has draft plan and can share it

Please present an English URL address or a website address that can give information on the relevant issues.

3. If you don't have a plan, could you identify the reason? (Multiple choices)

□ 1) lack of resources (information, experts, fund, etc.)

□ 2) never experienced serious spam related issues, so we don't feel any need

□ 3) Others: Please specify them

4. Have you measured the effectiveness of these initiatives? If so, what were your findings? If available, please provide data for the last three-year period, and describe your methodology for measuring the effectiveness.

5. To whom such initiatives mainly target (e.g., the population at large, children, elderly people, families, local communities, small and medium sized businesses, local authorities)?

6. Does your country have any private sector initiatives related to the education and awareness-raising on spam? If it does, please fill in the following information:

6-1. Existence of private sector initiatives: □ 1) Yes □ 2) No

6-2. URL:

6-3. Please provide the lists of activities of education and awareness-raising initiatives and date of establishment:

6-4. Name of organizations that implement each initiative

VI. International Cooperation

1. Has your country participated in any international cooperation initiatives on spam? If it does, please fill in the following information:

1-1. Existence of initiatives: ☐ 1) Yes ☐ 2) No

1-2. URL:

1-3. Names of initiatives and date of joining:

1-4. Name of government authority that handles related issues

2. If your country hasn't participated in any international cooperation initiatives on spam, does your country have any plan to make an international cooperation initiative ? If it does, please

fill in the following information:

2-1. Existence of plan: ☐ 1) Yes ☐ 2) No

2-2. preparation stage: ☐1) planning ☐ 2) research ☐ 3) drafting ☐ 4) under public consultation ☐ 5) under review before launch

2-3. If your country has draft plan and can share it

Please present an English URL address or a website address that can give information on the relevant issues.

3. If your country hasn't participated any international cooperation initiatives on spam and doesn't have any plans to create new one, does your country have any plan to join any existing one? If it does, please fill in the following information:

3-1. Existence of plan: □ 1) Yes □ 2) No

3-2. Please specify the existing international cooperation initiatives your country plans to join;

3-3. Expected date of joining;

4. If your country hasn't participated any initiatives or doesn't have any plans to join existing one, could you identify the reason? (Multiple choices)

□ 1) lack of resources (information, experts, fund, etc.)

□ 2) never experienced serious spam related issues, so we don't feel any need

□ 3) Others: Please specify them

5. If your country has any information, please provide examples of effective international initiatives to counter spam.

6. If your country has participated in any initiatives, have Memoranda of Understandings (MoUs) been established to implement these initiatives?

6-1. Existence of MoUs: □ 1) Yes □ 2) No

6-2. URL:

6-3. Names of MoUs and date of establishment:

6-4. Name of administrative institution that handles related issues

7. If your country has not participated in any international cooperation initiatives, how do you share information regarding spam-related issues with entities from other regions or countries?

8. If your country has participated in more than two international cooperation initiatives, which international cooperation initiatives have been most effective to you?

9. What challenges do you see to counter spam effectively cross-border?

10. If you have any, provide us examples of best practices in place and their effectiveness for the international cooperation in anti-spam area.

VII. List of experts

1. APT has a list of experts in ICT related matters. If you could recommend anyone who is an expert in legislative, technical, and operational aspects of spam related issues, please recommend him/her to us. (Please use the space below)

- Name:
- Job Title:
- Organization:
- E-mail:

2. Please provide your administration and country name.

The information you provide will be used for research only.

Added: In relation to anti-spam legislation and policy, please share any materials you may have.

Thank You!