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 139 Affiliate Members (as of November 2022) 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. Connectivity: Enhancing access and efficiency of digital infrastructure;
b. Innovation: Enabling conducive environments and harnessing the benefits of ICT;
c. Trust and Safety: Ensuring secure cyberspace, security and resilience through ICT;
d. Inclusion and Capacity Building: Promoting inclusiveness and enhancing digital skills; and
e. Collaboration and Partnership: Solidifying strategic cooperation with stakeholders.

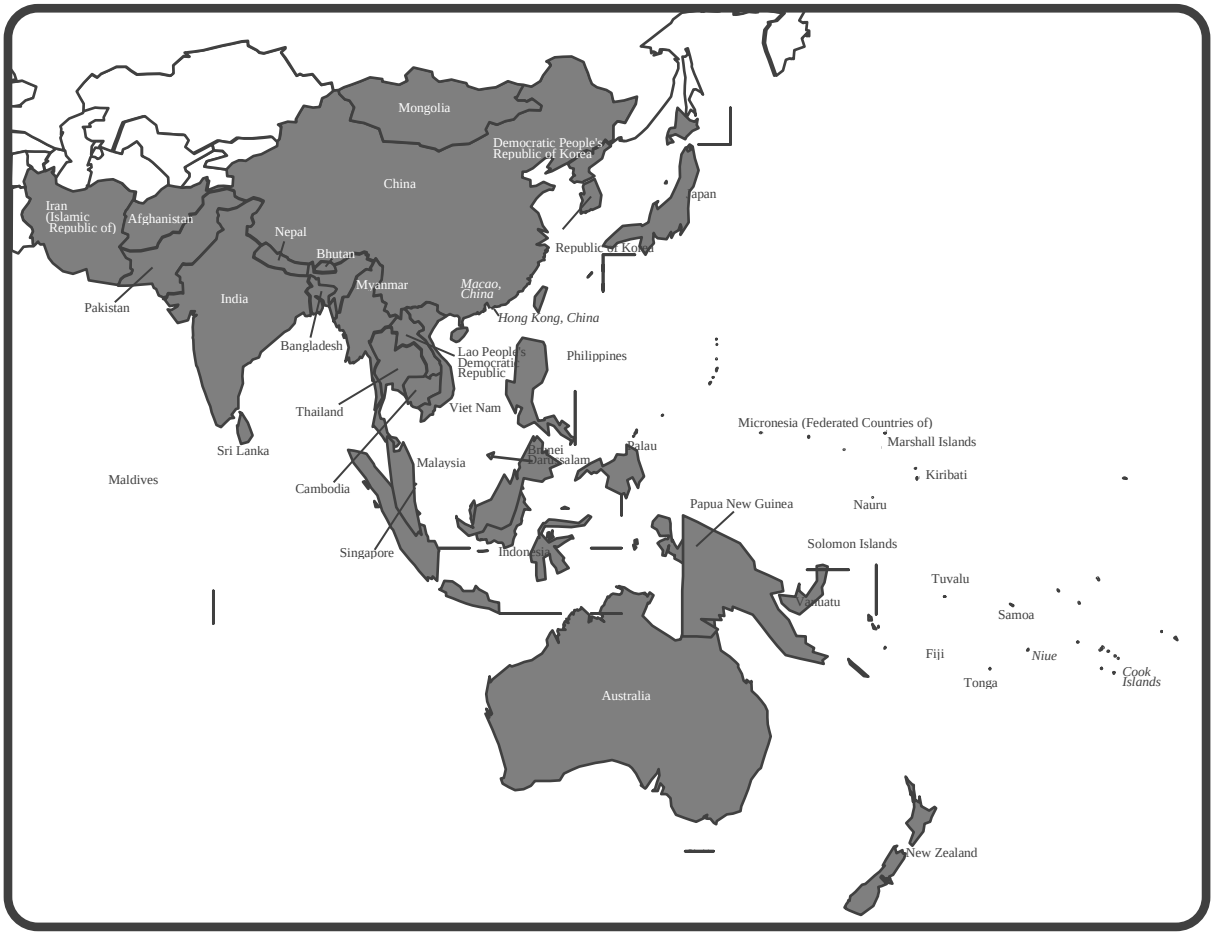


Fig: 38 Members and 4 Associate Members of the APT

ASIA-PACIFIC TELECOMMUNITY

Research Report

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

Research Period: March to December 2022

Korea Internet & Security Agency

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

Period: March to December 2022

Asia Pacific Telecommunity (APT)

Young Gyu Sin
Programme Officer

Shreya Pradhan
Assistant Project Coordinator

Korea Internet & Security Agency (KISA)

Jaesoon Gong
Manager

Dokyeong Kwon
General Researcher

Executive Summary

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 started out as electronic messages that advertised commercial products or services, has developed over the years, and now has a negative impact worldwide. It can be misleading, disrupt networks, and lead to various types of fraud that could be used as a platform for the spread of viruses and other malware.

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

However, in the Asia-Pacific region, there is no 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 andMC-45) of the APT in 2020 and 2021 respectively 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, above 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 considering possible measures to mitigate impact of 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 formation.

Since this research will be conducted for three years and 2022 is the second year of this

research project, in 2021 and 2022, research team conducted the survey on APT Members (including Associate Members)' anti-spam policy, issues, and legislation to figure out the current status of members regarding spam control. Also, research team conducted desk study based on journals, dissertations, and government documents that are publicly available to supplement the contents.

Regulations on spam e-mail and spam SMS/MMS (hereafter spam messages) are regulated by the same laws in most countries and have the same tendency. However, in some countries, different laws apply to spam e-mails and spam messages, so there are differences in regulatory framework.

The research result shows that regarding the regulation on spam e-mail, 9 (Australia, Cook Islands, Republic of Korea, Japan, Singapore, P.R.China, New Zealand, Hong Kong, Viet Nam) of the 25 countries studied during last two years have a comprehensive spam legislation. These countries are controlling spam by adopting an opt-in scheme (Australia, Cook Islands, Republic of Korea, Japan, P.R.China, New Zealand, Vietnam) or opt-out scheme (Singapore, Hong Kong). Regarding the regulation on spam messages, 9 (Australia, Cook Islands, Republic of Korea, Japan, Singapore, New Zealand, Hong Kong, Philippines, and Viet Nam) have a comprehensive legislation on spam messages. These countries have adopted an opt-in (Australia, Cook Islands, Republic of Korea, Japan, New Zealand, Philippines, Viet Nam) or opt-out (Singapore, Hong Kong) scheme to control spam messages. Australia, Cook Islands, Japan, Singapore, New Zealand, and Hong Kong have enacted separate spam e-mail/message laws. Republic of Korea, although not an individual spam e-mail/message law, has a separate section on spam in the Information and Communication Network Act to regulate spam e-mails/messages specifically and systematically. P.R.China has separate administrative regulations on spam e-mails and Philippines has enacted separate administrative regulations to regulate spam messages. Viet Nam has enacted enforcement decree to comprehensively regulate spam e-mails/messages.

As mentioned above, the anti-spam laws of APT Members are diverse, such as adopting opt-in or opt-out. As the opt-in and opt-out methods each have their own strengths and weaknesses, Members have established their spam regulation system by reflecting their own circumstances. However, for effective spam regulation, it is necessary to provide accurate sender information to the recipients regardless of opt-in/opt-out, and to include unsubscribe facility for opting out. In addition, if possible, it seems necessary to require the sender to indicate that the sent e-mail/message is an advertisement in the subject line, and to regulate the use of address harvesting software or the use of address lists automatically collected through it.

Regarding the spam policy of Members, the current status of policy measures to prevent

spam in Members are diverse in each of the country. In terms of technical measures, self-regulation, education and awareness-raising activities, and international cooperation activities, Members have established their spam policies by reflecting their own circumstances. However, as shown above, for effective spam control, it is necessary to prepare technical measures at the government level in addition to business-centered filtering, strengthen self-regulation, education, and awareness-raising activities, and seek to establish an international cooperative system and strengthen cooperative activities. In addition, it is noteworthy that many countries have recently shown a tendency to strengthen direct regulation of regulatory authorities rather than non-regulatory self-regulation.

However, if you gather the contents reviewed above, in the end, the spam control Act/policy should be flexibly developed to suit each country's situation. Each country will be able to come up with appropriate Act/policies by referring to the various examples studied in this research.

As we already reviewed above, many APT Members still do not have comprehensive legal systems for spam control. For spam email and SMS/MMS, only 9 out of the 25 countries studied this year have comprehensive anti-spam legislation. In addition, policy efforts to prevent spam are often somewhat insufficient, and only some countries have an international cooperation scheme to cooperate with other countries and international organizations.

It would be admirable if all Members could enact comprehensive spam control act, provide systematic and continuous policy support, and strengthen international cooperation efforts by establishing international cooperation system or participating in existing cooperation initiatives. However, due to economic, legal, and cultural diversity, some APT Members may find it difficult to enact comprehensive spam control laws, provide continuous policy support, or participate in international spam control initiatives.

Nevertheless, there is room for improvement for APT Members in the field of spam control. Although it is difficult to enact a comprehensive spam control law, efforts are needed to add new provisions that meet global standards or to revise some of the existing laws while maintaining the current legal system. By referring to the legal examples of leading countries in the Americas, Europe and Asia-Pacific region presented in this study, Members can make choices such as which new legal provisions to be added to existing laws or which parts of existing laws to be amended. The goals can be: 1) Providing accurate sender information, 2) Providing unsubscribe facility, 3) Prior consent, 4) Providing of labeling, 5) Prohibition of use of address harvesting software and automatically harvested address list.

The same is true in the field of spam control policies. 1) Providing technical support at the government level, 2) introducing self-regulation scheme, 3) strengthening education and awareness-raising activities, 4) strengthening international cooperation, etc. can be sought. If it is difficult to establish a new bilateral or multilateral cooperation system for spam control in relation to international cooperation, each country can participate in existing international cooperation initiatives such as UCENet. This can improve the level of spam control in society as a whole and increase trust on the Internet.

The ultimate goal of this research project is to find common elements and consider possible measures to mitigate impact of unsolicited commercial messages (spam) in the Asia-Pacific region. So, to this end, in 2023 research team plans to conduct (1) additional fact-finding surveys on the remaining Members that did not submit survey results during last two years, (2) analysis of problems/limitations of current international cooperation measures based on the results of the survey and desk study, (3) research to find common elements and consider possible measures to mitigate the impact of spam in the Asia-Pacific region.

From this point of view, this research plans to provide more detailed information on spam legislation, policies, and international cooperation systems in the future. Members can refer to this information to legislate or amend some existing laws related to spam, or to introduce policies and international cooperation measures that are appropriate to the situation/environment of each country. Members will be able to find the best option for their situation from among the various alternatives reviewed in this research.

In particular, APT plans to help Members through various work programmes such as Expert Mission and Training courses. The APT Secretariat will develop training courses in collaboration with KISA to provide information on global norms, trends, legislation and policy in the field of spam, which will be available to APT Members upon request basis in 2023. In addition, as part of the APT Expert Mission, APT Secretariat can also provide consulting on spam control legislation, policies, and international cooperation measures in collaboration with KISA when there is a request from Members. APT will continue to work with Members to ensure that these efforts continue.

Acknowledgements

Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in the Asia Pacific Region is the report paper as a result of in-house research fulfilled by Asia Pacific Telecommunity (APT).

This research report was conducted under Extra Budget Contribution-Korea (EBC-K) and approved as project 3.1.1 at the 44th and 45th Session of Management Committee (MC-44, 45) in 2020 and 2021.

This report was prepared under the overall leadership and guidance of Masanori Kondo, Secretary General of APT. Liu Ziping, Deputy Secretary General, provided valuable advice and comments. APT staff who contributed substantively include: Jongbong Park (Director, Project Development), Young Gyu Sin (Programme Officer), and Elisha Rajbhandari, Shreya Pradhan (Assistant Project Coordinator).

The report was coordinated by a core expert team of Korea Internet Security Agency (KISA) under the support and cooperation towards the APT programme with KISA. The following researchers provided inputs and basic structure: Jaesoon Gong, Minki Na (Manager) and Dokyeong Kwon, Kyeongsik Park (General Researcher).

The report benefited from the discussion at the APT Web Dialogues held on 24 September 2021 and 14 September 2022 virtually. This report also could be synchronized with the APT Members' who replied to Questionnaire in year 2021 and 2022.

Table of Contents

1. Introduction

1.1. Background of research

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 started out as electronic messages that advertised commercial products or services, has developed over the years, and now has a negative impact worldwide. It can be misleading, disrupt networks, and lead to various types of fraud that could be used as a platform for the spread of 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 the Asia-Pacific region, there is no 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 session of the Management Committee (MC-44) of the APT in 2020 approved to conduct research on "Collaborative Response Measures to Prevent Unsolicited Commercial Messages (Spam) in Asia Pacific Region" (MC44/OUT-18).

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.

1.2. Research method

Two methods were used to examine each country's spam legislation and policy scheme. The first method was to send the survey questionnaire "Questionnaire of APT research project on collaborative response measures to prevent unsolicited commercial messages (spam) in the Asia Pacific region" jointly prepared with KISA to the APT Members and receive the answers for analysis. Through this, accurate data on the current situation of each country could be collected. The second method was to conduct a desk study to find out the legislative cases of countries that are currently pursuing or promoting the enactment or revision of the Spam Act through data obtained from Members or found on the web, and to obtain data related to the policy scheme of countries regarding spam. Running these two approaches in parallel has allowed us to accurately understand individual countries' spam legislation and policy schemes.

1.3. The reason why sending of spam continues

In the case of spammers, mobile phones, e-mails, and Internet bulletin boards are used as a media of spam because they are easier to advertise and cost-effective than other means. Due to the nature of the medium, it is easy to conceal the identity of the sender, so it tends to be mainly used for advertisements (adult contents, gambling, drugs, loans, etc.) for secret illegal transactions that are prohibited by law.

In the case of telecommunication service providers, self-regulation efforts are insufficient, such as neglect of supervision of spammers' service use and lack of investment and publicity to build a spam blocking system.

Users neglect the management of their own personal information, and there are many cases in which users provide their own information to a person who are sending spam. There is a lack of awareness of the spam blocking function and service, and users are normally not active in using response measures such as reporting to telecommunication service providers or government authority.

In this way, the problems of spammers, telecommunication companies, and users are not resolved, so spam continues even though it has been one of the long-lasting issues in ICT.

1.4. Damage from spam

The increase in spam is a representative factor that threatens the convenience, reliability, and efficiency of information and communication technology. Spam causes mental damage such as inconvenience and irritation to recipients and causes unnecessary social costs such as waste of time and reduced productivity. In addition, the cost is passed on to the telecommunication service provider by aggravating network resource consumption in message transmission/storage.

2. Global trends

2.1 Trends in the developed countries[1]

The approaches of four jurisdictions in America and Europe– the United States of America

[1] ACMA, “Unsolicited Communications Research; A Study of International Best Practice”, https://www.acma.gov.au/sites/default/files/2019-08/ACMA-UC-Research-Findings-Report-May-2018.pdf

(USA), Canada, France, and Germany- to unsolicited messages management are most advanced and meaningful to other countries. There are three key components to the approaches that governments are taking to manage unsolicited messages in their jurisdictions, as below:

- legislation and regulation that underpins governments' management of the sending of unsolicited messages;
- effective enforcement of the legislation and regulation that exists; and
- non-legislative activities such as preventative measures to reduce the number of unsolicited messages reaching consumers, and public and industry educational activities.

2.1.1. United States of America

In the US, email spams are regulated by the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act (2003), and SMS/MMS spams are controlled by Telephone Consumer Protection Act of 1991 and CAN-SPAM (2003). Telephone Consumer Protection Act of 1991, Do-Not-Call Implementation Act of 2003, Truth in Caller ID Act 2009 and Telemarketing Sales Rules (TSR) are altogether regulating phone call spams, and Junk Fax Prevention Act of 2005 regulates Fax spams. In addition to the federal laws above, many states also have their own relevant acts which are managed at the state level.

Responsibility for managing unsolicited messages is split between the Federal Trade Commission (FTC), the Federal Communications Commission (FCC) and each of the 50 states. The FTC promotes competition and protects and educates consumers on their rights and responsibilities, and the FCC implements and enforces the USA's communications law and regulations.

In addition, many states have their own sets of unsolicited messages regulations, which overlap with federal responsibilities. Many of the state-based operations pre-date the federal operations, explaining this overlap. For example, both federal and state Do Not Call registers. Marketers are required to consult both lists.

The FTC, FCC and states frequently collaborate on target selection and enforcement issues. They also share information and collaborate on public-facing roundtables and workshops, such as a policy forum on illegal robocalls, and a consumer expo and policy forum on highlighting the two agencies' and industry partners' efforts in combatting robocalls. The FTC, FCC and states engage regularly, particularly through (at least monthly) conference calls with state Attorneys General. The USA's Department of Justice also participates in the monthly calls, as does the Canada's CRTC. The FTC also sometimes files joint law enforcement cases with the FCC and state Partners.

2.1.2. Canada

In Canada, email spams and SMS/MMS spams are regulated by the Act to Promote the Efficiency and Adaptability of the Canadian Economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) (more commonly known as Canada's Anti-Spam Legislation [CASL]2014). Canada's Anti-Spam Legislation (CASL) 2014 has been designed as ″technology neutral", covering all forms of what it classifies as "electronic" Communication. Unsolicited Telecommunications Rules (UTR) are regulating phone call spams and Fax spams.

Responsibility for enforcing the "unsolicited" aspect of unsolicited communications falls to the Canadian Radio-television and Telecommunications Commission (CRTC). Innovation, Science and Economic Development Canada (ISED) – the parent department of the CRTC – is responsible for policy-setting.

While the CRTC has the primary role in the enforcement of unsolicited communications legislation and regulation, the content of messages can involve other agencies, such the Competition Bureau (CB), the Office of the Privacy Commissioner of Canada (OPC) and the Royal Canadian Mounted Police (RCMP).

The CRTC operates the Spam Reporting Centre, through which consumers can report violations of the CASL for the CRTC to act against. The CRTC also operates a national Do Not Call (DNC) register, through which consumers can report violations of the UTR.

2.1.3. France

In France, the Law of June 21, 2004, for Confidence in the Digital Economy regulates email spam, SMS/MMS spam, phone call spam, and fax spam.

Responsibility for managing unsolicited communications falls to the Commission Nationale de l'Informatique et des Libertés (CNIL).

The CNIL also manages the outsourcing of the Do Not Call Register. Currently the DNC register, "BLOCTEL", is managed by a consortium. The register, in operation since 2016, has taken a much heavier approach to enforcement (through CNIL and the Directorate-General for Competition, Consumer Affairs and Fraud Control [DGCCRF]) than the previous register ("PACITEL") did, under which breaches of the register were not punished. The CNIL's efforts are also supplemented by industry initiatives that collect SMS/MMS and email spam, and telephone spam. The CNIL has endorsed some of these initiatives – including Signal Spam (email) and 33700 (voice and SMS/MMS) –and advertises these as reporting channels for consumers.

There is some overlap between the CNIL's responsibilities and the Ministère de l'Intérieur

(Ministry of the Interior) and the DGCCRF. The Ministère de l'Intérieur operates a separate government "phishing" reporting portal, which accepts direct reports of criminal misbehavior online, including malicious emails. The DGCCRF overlaps with the CNIL's sphere of operation when there is fraud involved in a case.

The Law of June 21, 2004, for Confidence in the Digital Economy was introduced in response to the EC's ePrivacy directive in 2003, bringing French law in line with the new European Union standard.

2.1.4. Germany

In Germany, the Telecommunications Act (also known as Telekommunikationsgesetz or TKG) and Unfair Competition Act (also known as Gesetz gegen den unlauteren Wettbewerb or UWG) regulate email spam, SMS/MMS spam, phone call spam, and fax spam.

The responsibility for managing unsolicited messages falls almost entirely to the Bundesnetzagentur (also known as the Federal Network Agency or the BNetzA), a higher federal authority which is subject to the legal and professional supervision of the Federal Ministry of Economics and Energy.

The BNetzA has a very wide remit and is responsible for electricity and gas, post, rail and communications network planning and management. Its unsolicited messages responsibilities include:

- enforcing the TKG with regard to combating number misuse;
- enforcing the TKG with regard to combating spam, including SMS/MMS, and email spam. The TKG is involved taking action against email spam only when the email communication is connected to a phone number (i.e. where there is a phone number within an email whereby the sender can be contacted); and
- enforcing the UWG as it applies to unreasonable disturbance by fax or SMS spam.

Germany has a general ban on direct telephone marketing to consumers, so does not operate a Do Not Call list – in other words, consumers must "opt-in" with an organization to receive marketing calls.

Several other non-government organizations contribute to Germany's defense against email spam, complimenting the BNetzA's activities.

2.1.5. European Union

In addition to jurisdiction-specific approaches, the European Union (of which France and Germany are members) has two key documents that guide member states' regulation of unsolicited emails, being:

- the EU ePrivacy Directive 2002 – this directive discourages all email marketing unless three criteria are satisfied; 1) explicit or implied consent is given, 2) contact details for the sender are included in the email and 3) an unsubscribe link is included. The implementation of the directive is the responsibility of EU members; and
- the EU General Data Protection Regulation (GDPR), which is due to be introduced and legally binding from 25 May,2018 and supersede the directive. Unlike the directive, the GDPR will be legally binding for EU members. The key features of the GDPR are:

    - mandated collection of explicit consent, which will be applied retrospectively. This means that individuals who have implicitly but not explicitly granted consent to receive marketing communications (in jurisdictions where that is currently allowed) can no longer be contacted;
    - a tiered approach to fines, with the most serious offences (failure to collect appropriate consent) attracting fines of up to four percent of an organization's global annual turnover or €20 million – whichever is greater.
    - extending the jurisdiction of the GDPR (and removing ambiguity in the directive) to include all companies controlling and processing data of individuals residing in the EU. This includes companies that are based outside the EU but interact with EU residents' data –such companies will also need to appoint a representative in the EU where they do not have one already.

2.2. International cooperation activities

2.2.1. Convention on Cybercrime (2001)

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It was opened for signature on 23 November, 2001, and as of December 2020, 65 states have ratified the convention.

Even though this convention does not regulate spam or unsolicited commercial messages with direct provisions, this convention regulates the offences against the confidentiality, integrity and availability of computer data and systems. Also, it stipulates the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation, and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation. So, it can be considered that this convention includes the basic provisions and spirit to fight against computer-related crimes and to promote user protection in cyber world.

2.2.2. EU e-privacy directive[2] (2002)

Related to privacy protection of subscribers EU e-Privacy Directive has some provisions related to the unsolicited commercial messages. They are about the prior explicit consent of the recipients, opportunity to object (to receive), prohibit the use of false identity/false return address, etc.

Article 13

Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

2.2.3. London Action Plan (2004)

On October 11, 2004, government and public agencies from 27 countries responsible for enforcing laws concerning spam met in London to discuss international spam enforcement

[2] EU Directive 2002/58/EC, Directive on Privacy and Electronic Communications

cooperation. At this meeting, a broad range of spam enforcement agencies, including data protection agencies, telecommunications agencies, and consumer protection agencies, met to discuss international spam enforcement cooperation. Several private sector representatives also collaborated in parts of the meeting.

Global cooperation and public-private partnerships are essential to spam enforcement, as recognized in various international fora. Building on recent efforts in organizations like the Organization for Economic Cooperation and Development (OECD) and the OECD Spam Task Force, the International Telecommunications Union (ITU), the European Union (EU), the International Consumer Protection Enforcement Network (ICPEN), and the Asia-Pacific Economic Cooperation (APEC), the participants issue this Action Plan. The purpose of this Action Plan is to promote international spam enforcement cooperation and address spam-related problems, such as online fraud and deception, phishing, and dissemination of viruses. The Participants also open the Action Plan for participation by other interested government and public agencies, and by appropriate private sector representatives, to expand the network of entities engaged in spam enforcement cooperation.

The content of London Action Plan is as follows:

A. The participating government and public agencies (hereinafter "Agencies"), intend to use their best efforts, in their respective areas of competence, to develop better international spam enforcement cooperation, and intend to use their best efforts to:

1. Designate a point of contact within their agency for further enforcement communications under this Action Plan.

2. Encourage communication and coordination among the different Agencies that have spam enforcement authority within their country to achieve efficient and effective enforcement, and to work with other Agencies within the same country to designate a primary contact for coordinating enforcement cooperation under this Action Plan.

3. Take part in periodic conference calls, at least quarterly, with other appropriate participants to:

a. Discuss cases.

b. Discuss legislative and law enforcement developments.

c. Exchange effective investigative techniques and enforcement strategies.

d. Discuss obstacles to effective enforcement and ways to overcome these obstacles.

e. Discuss undertaking, as appropriate, joint consumer and business education projects addressing problems related to spam such as online fraud and deception, phishing, and dissemination of viruses. Such projects could include educational efforts addressing conditions facilitating the anonymous delivery of spam, such as the use of open relays, open proxies, and zombie drones.

f. Participate as appropriate in joint training sessions with private sector representatives to identify new ways of cooperating and to discuss spam investigation techniques.

4. Encourage dialogue between Agencies and appropriate private sector representatives to promote ways in which the private sector can support Agencies in bringing spam cases and pursue their own initiatives to fight spam.

5. Prioritize cases based on harm to victims when requesting international assistance.

6. Complete the OECD Questionnaire on Cross-border Enforcement of Anti-Spam Laws, copies of which may be obtained from the OECD Secretariat.

7. Encourage and support the involvement of less developed countries in spam enforcement cooperation.

The participating Agencies intend to keep information shared in the context of this Action Plan confidential when requested to do so, to the extent consistent with their respective laws. Similarly, the participating Agencies retain the right to determine the information they share under this Action Plan.

B. The participating private sector representatives (whether as a group or through its members) intend to use their best efforts to develop public-private partnerships against spam and to:

1. Designate a single spam enforcement contact within each organization, who would coordinate with spam enforcement agencies on requests for enforcement-related assistance

2. Work with other private sector representatives to establish a resource list of individuals within particular sectors (e.g., Internet service providers, registrars, etc.) working on spam enforcement.

3. Participate as requested and appropriate in segments of the periodic conference calls described in paragraph A.3 above for the purpose of assisting law enforcement agencies in bringing spam cases. (Because some calls will be focused solely on law enforcement matters, private sector representatives will participate only in selected calls.) In these conference calls, the participating private sector representatives intend to use their best efforts to:

a. Report about:

i. Cases involving spam or related matters.

ii. New technology and trends in email and spam.

iii. New ways of cooperating with Agencies.

iv. Obstacles to cooperation with Agencies and within the private sector.

v. General data on spam and on-line fraud as an early warning mechanism for Agencies.

b. Assist as appropriate in training sessions on subjects such as the latest spam

investigation techniques to help Agencies in investigating and bringing spam cases.

In order to prevent inappropriate access to information, a private sector representative may be excluded from participating in all or a portion of the periodic conference calls described above if a participating Agency objects.

4. Work cooperatively with Agencies to develop the most efficient and effective ways to frame requests for information. For this purpose, each participating private sector representative intends to use best efforts to compile written responses to the following questions:

a. What kind of information do you provide about potential spammers to domestic law enforcement agencies and under what circumstances?

b. What kind of information would you provide about potential spammers to foreign law enforcement agencies and under what circumstances?

c. How do you recommend that spam enforcement agencies submit requests for assistance to you?

C. In order to begin work pursuant to this Action Plan, the U.K. Office of Fair Trading and the U.S. Federal Trade Commission intend to use best efforts to:

1. Collect and disseminate information provided pursuant to this Action Plan, including points of contact, notifications from new Participants of their willingness to endorse this Action Plan, and responses to questionnaires, in cooperation with the OECD.

2. Set up the conference calls mentioned in paragraph A.3.

3. Provide a contact for further communications under this Action Plan.

The participating Agencies expect that this procedure may be modified at any time.

D. This Action Plan reflects the mutual interest of the Participants in the fight against illegal spam. It is not intended to create any new legally binding obligations by or amongst the Participants, and/or require continuing participation.

Participants to this Action Plan recognize that cooperation pursuant to this Action Plan is subject to their laws and their international obligations, and that nothing in this Action Plan requires the Participants to provide confidential or commercially sensitive information.

Participants in this Action Plan intend to use best efforts to share relevant findings of this group with the OECD Spam Task Force and other appropriate international groups.

This Action Plan is meant to be a simple, flexible document facilitating concrete steps to start working on international spam enforcement cooperation. It is expected that the collective work program under this Action Plan may be refined, and if necessary, changed by the participants, as new issues arise.

Additional Agencies, and private sector representatives as defined below, may endorse and take part in this Action Plan as long as no Agency that has endorsed this Action Plan objects.

"Private sector representatives" invited to participate in this Action Plan include financial institutions, Internet service providers, telecommunications companies, information security software providers, mobile operators, courier services, commercial mail receiving agencies, industry membership organizations, consumer organizations, payment system providers, credit reporting agencies, domain name registrars and registries, and providers of alternative dispute resolution services.

2.2.4. Anti-spam toolkit (OECD, 2006)

In view of the potential for economic and social harm of spam, and the potential for further problems as a result of the convergence of communication technologies, the ICCP(Information, Communications and Computer Policy) Committee, in consultation with the CCP(Committee on Consumer Policy), endorsed in April 2004 the proposal for the creation of a horizontal ad hoc “Joint ICCP-CCP Task Force on Spam” to assist in the further conduct and co-ordination of the work on spam and obtain a more rapid consensus on a policy framework to tackle spam issues. The creation of the Task Force on Spam, as a joint subsidiary body of these Committees, was approved by the OECD Council.

The OECD Anti-Spam Toolkit was developed in the framework of the OECD Task Force on spam and includes a package of recommended policies and measures addressing regulatory approaches, enforcement co-operation, industry driven activities, technical solutions, education and awareness initiatives, spam measures, and international co-operation and exchange. The Toolkit was declassified on 29 March 2006 by the ICCP committee and the CCP, and the Enforcement Recommendation was adopted by the Council at its meeting on 13 April 2006. The Task Force’s mandate ends in June 2006.

Contents of toolkit

- Anti-spam regulation
- Anti-spam enforcement
- Anti-spam technologies
- Education and awareness
- Co-operation partnership against spam
- Spam measurement
- Global co-operation

2.2.5. UCENet[3](2016)-from London Action Plan network to UCENet

UCENet was started in 2016 by the members of London Action Plan (LAP)*. As a result of consultation with LAP members in 2016, to better reflect the aims of the LAP network and the type of work that the LAP does, agreement was obtained to change the name of the network to the Unsolicited Communications Enforcement Network (UCENet) as of 09 September 2016. This date was chosen as it proceeded the annual LAP conference that in 2016 was held in Paris. Whilst the LAP served members and the broader internet community since its inception in 2004, the internet has changed, and the new name was chosen to reflect the network going forward.

Members

- *Regulatory and Enforcement authorities (28):* Australia, Belgium, Brazil, Canada, Chile, China, Denmark, Finland, Hong Kong, Hungary, Ireland, Japan, Latvia, Lithuania, Malaysia, Mexico, Netherlands, Nigeria, Norway, Portugal, Korea, South Africa, Spain, Sweden, Switzerland, Taiwan, UK, USA
- *Industry Participants (27):* ISOC of China, Telefonica, McAfee, etc.

Structure of Organization

- UCENet Executive Committee, composed of the Co-chairs, plus a minimum of four members from other authorities or agencies, with attention given to geographic diversity and representation, and responsible for providing strategic direction and oversight of UCENet activities.
- The Secretariat provides administrative, technical and operational support to the UCENet Executive Committee, the UCENet working groups.
- Working groups contribute significantly to the cooperative program under UCENet.

Activities

- Sharing information and intelligence to identify risks and opportunities for enforcement action and/or prevention.
- Sharing of effective intelligence and investigative techniques and enforcement strategies.
- Exploration of similarities and differences in procedural, substantive, and evidentiary

[3] Unsolicited Communications Enforcement Network

rules to address challenges to cooperation.

- Cooperation with other organizations or networks involved with related activities.
- Sharing insights with countries implementing new regulatory regime programs.
- Posting relevant content to the UCENet website, such as enforcement and compliance outcomes and initiatives.

2.2.6. ITU-D Study Group Research (2018~)

According to the ITU-D Buenos Aires Action Plan, ITU-D Study Group 1is conducting research on "Unsolicited Commercial Communications – an overview of challenges and strategies (2018-2021 ongoing)". This research brings an overview of challenges linked to nuisance and fraudulent calls and text messages and the strategies adopted by different countries to tackle the problem. After contextualizing the problem, this research showcases approaches from different countries. In general, a situation involving four stakeholders is considered, namely: telecommunication operators, market players selling their services or products, telecommunication regulators, and consumers. The specific approaches for each stakeholder are discussed with examples.

2.2.7. WTO e-commerce negotiations (2019~)

WTO negotiations on trade-related aspects of electronic commerce were launched in Davos, Switzerland, in January 2019 with the participation of 76 members. The number of participating members now stands at 86. Participating members are seeking to achieve a high-standard outcome that builds on existing WTO agreements and frameworks with the participation of as many WTO members as possible.

The negotiations are based on text proposals submitted by WTO members and are conducted through a combination of plenary, focus group and small group meetings. Currently, the discussions are covering six main themes: enabling e-commerce; openness and e-commerce; trust and e-commerce; cross-cutting issues; telecommunications; and market access.

E-commerce negotiations' members finalized "clean text" on unsolicited commercial messages (Feb 2021).

At the first meeting of the year on e-commerce negotiations, held on 5 February 2021, co-convenor Ambassador George Mina (Australia) commended WTO members for finalizing a clean negotiating text on the issue of unsolicited commercial messages, otherwise known as spam. Ambassador Mina said that 2021 is a critical year for the e-commerce initiative and

stressed that members need to intensify the pace of talks to deliver on the goal of substantial progress by the 12th Ministerial Conference (MC12) due to take place this year.

The facilitator of the small group discussion on "spam", Seojin Yang (Republic of Korea), reported that the group has finalized a clean text, which aims at minimizing spam messages in e-commerce. Ambassador Mina hailed this is as a milestone in the negotiations. It is the result of members' creativity, flexibility and efforts to strike a balance, he said.

The clean negotiating text prepared by this small group was supposed to be discussed at the 12th Ministerial Conference (MC12) this year, but the meeting date was postponed.

2.2.8. RCEP Agreement[4]

The Regional Comprehensive Economic Partnership (RCEP) Agreement, signed on November 15, 2020, contains an unsolicited commercial message clause. According to this, the State party is obliged to establish a consent system and recourse method to protect users from spam messages.

Art.12.9: Unsolicited Commercial Electronic Messages

1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that:

(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to stop receiving such messages;

(b) require the consent, as specified according to its laws and regulations, of recipients to receive commercial electronic messages; or

(c) otherwise provide for the minimization of unsolicited commercial electronic messages.

2. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages who do not comply with its measures implemented pursuant to paragraph 1.

3. The Parties shall endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

(fn9) Cambodia, Lao PDR, and Myanmar shall not be obliged to apply this paragraph for a period of five years after the date of entry into force of this Agreement. Brunei Darussalam shall not be obliged to apply this paragraph for a period of three years after the date of entry into force of this Agreement.

As can be seen from this article, the Agreement imposes an obligation to adopt and maintain

[4] Australia, Brunei, Cambodia, China, Indonesia, Japan, Laos, Malaysia, Myanmar, New Zealand, the Philippines, Singapore, South Korea, Thailand, and Vietnam signed the RCEP agreement.

measures relating to spam messages.

- Paragraph 1 provides that with respect to spam messages, each Party (a) requires suppliers to facilitate the ability of recipients to stop receiving such messages; (b) requires to obtain consent of recipients, and (c) requires minimization of spam.
- Since all the measures listed here are linked with 'or', the Parties do not have an obligation to implement all measures mentioned in paragraph 1, and, paragraph 1 (c) 'minimization of spam' is specified so that each Party can autonomously choose the fulfillment of the obligations of this article according to its legal system and circumstances.

The agreement also imposes an obligation to provide a recourse method for non-compliance.

- Paragraph 2 stipulates that each Party is obliged to provide users with a means of recourse to respond to service providers who fail to comply with measures introduced or maintained for compliance with Paragraph 1.
- Paragraph 2 is silent on what means of recourse should be provided, so a State party can choose an effective means of implementation that conforms to its legal system and policy situation. Recourse for damages through general civil litigation, spam reporting to regulatory agencies, criminal punishment and fines for negligence can be possible recourse methods.

In addition, paragraph 3 imposes an obligation to strive for cooperation.

- Paragraph 3 stipulates the duty of effort for cooperation between the parties in the regulation of spam mail, but it simply requires efforts for cooperation in “appropriate cases of mutual concern” without mentioning the method and procedure of cooperation.
- As there is no specific requirement regarding the subject, method, procedure, etc. of cooperation, a separate implementation action is not required for the obligation.

3. Current Status related to spam by country

3.1. Review of cases by country

3.1.1. Australia

A. Definition of spam

In Australia, Spam Act defines that spam is an unsolicited commercial electronic message.

Section 6 of the Spam Act 2003 (national law) 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

Types of spam

In Australia, section 5 of the Spam Act further defines that an electronic message is a message sent using an internet carriage service to an electronic address in connection with an email account, instant messaging account, telephone account or a similar account. As such, in Australia, spam law predominantly concerns email, SMS and instant message. There are separate laws for voice calls in Australia, under the Do Not Call Register Act 2006. The Australia Communications and Media Authority (ACMA) identifies spam via a variety of sources, mainly via complaints from consumers.

When assessing spam complaints, the ACMA identifies the relevant sector/industry or issue to assist with identifying trends in spam activity and identify areas for priority action. However, the ACMA does not generally publish this information, and the categories can change from time to time.

B. Current status for spam response

The ACMA does not quantify spam as a percentage of all email, SMS or instant messaging

traffic. The ACMA regularly published information on the number of spam complaints from the public, which can be accessed on their website: "Action on spam and telemarketing[5]."

Telemarketing and spam emails or SMS messages are an issue for many Australians. ACMA protect the public by promoting and enforcing the law.

ACMA provide the Do Not Call Register (DNCR), promoting responsible industry practice and monitor and enforce compliance with the law; Spam Act 2003 and Do Not Call Register Act 2006.

ACMA activities depend on the risk of harm and the impact on consumers. ACMA can:

- provide compliance information to industry
- contact businesses to warn them when ACMA receive complaints
- investigate serious or ongoing problems
- take enforcement action where warranted

ACMA rely on information from different sources, including complaints, reports, industry feedback and information from international regulators.

ACMA publish quarterly reports of the actions they have taken as a result of their investigations.

1) Action on spam and telemarketing: April to June 2021

Key actions
Kalkine financial services businesses paid **$352,200 in ACMA-given penalties** for spam and telemarketing breaches
Over $2.5 million in penalties paid in the last 2 years

[5] ACMA, "Action on spam and telemarketing", https://www.acma.gov.au/action-spam-and-telemarketing

formally warned 4 businesses for breaching spam and telemarketing laws

gave **1,030 compliance alerts** to businesses

agreed to collaborate with the **Federal Communications Commission (USA)** to address unsolicited communications, including scams

2) Action on spam and telemarketing: January to March 2021

Key actions

55 million scam calls blocked under new rules

$310,800 penalty paid by Kogan Australia for spam breaches

$79,800 penalty paid by Telco First Pty Ltd for spam breaches

Court-enforceable commitments accepted from Seek the Deal Pty Ltd, Kogan Australia and Telco First

1,089 compliance alerts given to businesses

$2,194,500 in paid penalties by businesses in the last 2 years

Source: *https://www.acma.gov.au/*

3) ACMA priorities

Regarding spam issues, unlawful financial service marketing and phone scams were a focus in 2020–21 and will continue to be in 2021–22.

(A) Unlawful financial services marketing

ACMA continued to directly engage with businesses marketing financial products and services to alert them to compliance issues during the second quarter in 2021.

ACMA finalized 6 investigations:

- Kalkine Pty Ltd and Kalkine Media Pty Ltd paid penalties of $352,200 for breaching telemarketing and spam laws. ACMA also accepted court-enforceable undertakings from both businesses.
- ACMA formally warned Lastminuteloan.com Pty Ltd and IPF Digital Australia Pty Ltd (t/a Credit24) for breaching spam laws.
- ACMA formally warned Martin and Hunt Pty Ltd and Chase Edwards & Associates Pty Ltd for breaching telemarketing laws.

(B) Combating phone scams

ACMA are taking the fight to scammers to disrupt their activities and protect Australians. During the second quarter in 2021, ACMA:

- Issued formal warnings to 3 telcos (Telstra, Medion and Optus) for breaching identity verification rules. These rules are made to protect consumers from identity theft.

- ACMA agreed to collaborate with the Federal Communications Commission (USA) to combat unlawful robocalls, unsolicited texts and phone scams. This will include the sharing of intelligence, and coordination of investigation and enforcement activities.
- Warned consumers about scammers targeting the COVID-19 vaccination rollout.
- Worked behind the scenes with government agencies and telcos to disrupt SMS scams targeting government messaging about COVID-19.
- Provided de-identified complaint data to telcos to help them identify and block scam calls.

4) Key compliance issues: Consent to send messages

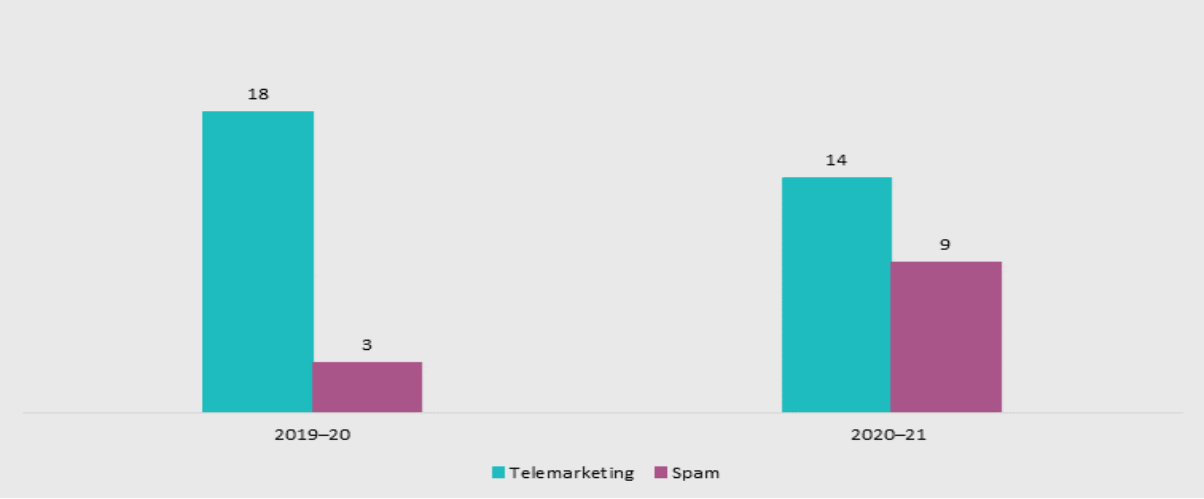
The impact of COVID-19 on traditional bricks and mortar businesses and the large number of Australians working from home over the past year has seen an increase in electronic marketing and online sales platforms.

This has contributed to an increase in spam complaints to the ACMA. These are up 63% from 2019–20.

Businesses must not undertake e-marketing such as email, SMS, and instant messaging without consent. Where they have consent, they must be able to prove it with accurate and clear records.

Entities need to remember that they still have compliance obligations when relying on others to send messages on their behalf. This includes when purchasing contact lists.

5) Finalized investigations



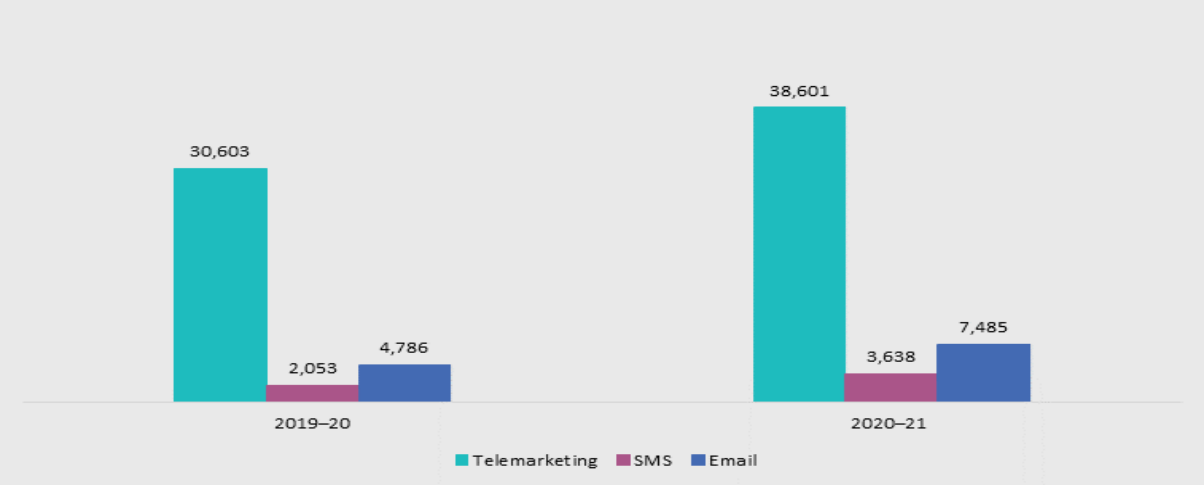
Source: https://www.acma.gov.au/

6) Complaints

Consumer complaints directly inform ACMA actions and help them identify issues and trends. ACMA also provide de-identified complaint data to telcos to help them identify and block scam calls.

In the June 2021 quarter:

- 37.5% of telemarketing and 18.8% of spam complaints were about scams.
- The most common complaints were about the financial services, retail, solar telemarketing, and gambling industries.
- 40.4% of complaints about telemarketing did not contain enough detail to identify the caller.



Note: ACMA also received 12 complaints about commercial instant messages in June quarter.

7) Compliance alerts

ACMA alert businesses about potential compliance issues raised in complaints (where ACMA can identify the business). ACMA provide details to the business when the person complaining has given them permission. If the issues continue, ACMA may investigate. One alert can relate to several issues or complaints.

Source: https://www.acma.gov.au/

C. Legislation related to spam

1) Key concepts

(1) commercial electronic message

Commercial electronic message is an electronic message, where, having regard to:

(a) the content of the message; and

(b) the way in which the message is presented; and

(c) 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 of the purposes, of the message is:

(d) to offer to supply goods or services; or

(e) to advertise or promote goods or services; or

(f) to advertise or promote a supplier, or prospective supplier, of goods or services; or

(g) to offer to supply land or an interest in land; or

(h) to advertise or promote land or an interest in land; or

(i) to advertise or promote a supplier, or prospective supplier, of land or an interest in land; or

(j) to offer to provide a business opportunity or investment opportunity; or

(k) to advertise or promote a business opportunity or investment opportunity; or

(l) to advertise or promote a provider, or prospective provider, of a business opportunity or investment opportunity; or

(m) to assist or enable a person, by a deception, to dishonestly obtain property belonging to another person; or

(n) to assist or enable a person, by a deception, to dishonestly obtain a financial advantage from another person; or

(o) to assist or enable a person to dishonestly obtain a gain from another person; or

(p) a purpose specified in the regulations.

(2) Australian link

A commercial electronic message has an Australian link if, and only if:

(a) the message originates in Australia; or

(b) the individual or organisation who sent the message, or authorised the sending of the message, is:

(i) an individual who is physically present in Australia when the message is sent; or

(ii) an organisation whose central management and control is in Australia when the message is sent; or

(c) the computer, server or device that is used to access the message is located in Australia; or

(d) the relevant electronic account holder is:

(i) an individual who is physically present in Australia when the message is accessed; or

(ii) an organisation that carries on business or activities in Australia when

the message is accessed; or

(e) if the message cannot be delivered because the relevant electronic address does not exist—assuming that the electronic address existed, it is reasonably likely that the message would have been accessed using a computer, server or device located in Australia.

(3) designated commercial electronic message

The designated commercial electronic message is a message that has factual information, the sending of the message is authorised by Government bodies, political parties and charities, and educational institution, etc.

- (Factual information) an electronic message is a designated commercial electronic message if:

(a) the message consists of no more than factual information (with or without directly related comment) and any or all of the following additional information:

(i) the name, logo and contact details of the individual or organisation who authorised the sending of the message;
(ii) the name and contact details of the author;
(iii) if the author is an employee—the name, logo and contact details of the author's employer;
(iv) if the author is a partner in a partnership—the name, logo and contact details of the partnership;
(v) if the author is a director or officer of an organisation—the name, logo and contact details of the organisation;
(vi) if the message is sponsored—the name, logo and contact details of the sponsor;
(vii) information required to be included by section 17;
(viii) information that would have been required to be included by section 18 if that section had applied to the message; and

- (Government bodies, political parties and charities) an electronic message is a designated commercial electronic message if:

(a) the sending of the message is authorised by any of the following bodies:

(i) a government body;

(ii) a registered political party;

(iii) a registered charity; and

(b) the message relates to goods or services; and

(c) the body is the supplier, or prospective supplier, of the goods or services concerned.

- (Educational institution) an electronic message is a designated commercial electronic message if:

(a) the sending of the message is authorised by an educational institution; and

(b) either or both of the following subparagraphs applies:

(i) the relevant electronic account holder is, or has been, enrolled as a student in that institution;

(ii) a member or former member of the household of the relevant electronic account holder is, or has been, enrolled as a student in that institution; and

(c) the message relates to goods or services; and

(d) the institution is the supplier, or prospective supplier, of the goods or services concerned.

2) Contents of spam legislation

(1) Regulatory framework

Basically, the Australian government has an opt-in system for spam emails and spam messages (SMS/MMS). Regarding voice calls, there is a separate regulation under the Do-Not-Call Register Act of 2006, which prohibits calls to the phone numbers registered in the Do-Not-Call Register.

It is illegal to send or cause unsolicited commercial electronic messages to be sent under the 2003 Australian Spam Act. The Act covers e-mail, instant messaging, SMS and MMS of a commercial nature. The Act does not cover fax, Internet pop-up or voice telemarketing.

Australia is one of the pioneers and leaders in the Asia Pacific region when it comes to anti-spam legislation. Australia is also one of the few countries in Asia that has successfully caught

spammers in their country and enforced anti-spam law. Here's a brief overview of Australia's spam law.

The Spam Act does not contain bulk requirements (sending many messages during certain time limits) and governs a wide range of commercial messages. Commercial electronic messages are essentially electronic messages whose purpose is to promote or offer the provision of goods or services. In order to avoid violating the law, electronic commerce message senders must (1) obtain the recipient's consent, (2) provide accurate sender information, and (3) include an unsubscribe facility.

Recipients can expressly consent to receiving commercial electronic messages, or their consent may be inferred from their actions, business, or other relationships. Australia's spam law precedent showed that if there is a pre-existing relationship between email sender and recipient, and the email relates to a product or similar product that has already been purchased by a recipient, and the recipient does not notify that he/she does not wish to receive the email, the consent can be inferred. It is also important that consent provided under that Act can be revoked. The Act provides that if the recipient sends a request to the sender that the recipient no longer wishes to receive commercial electronic messages from the sender, consent shall be deemed to be withdrawn within five business days of receipt of the opt-out request.

(Consent) 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 (opt-in).

(Commercial electronic messages must include accurate sender information) A person must not send, or cause to be sent, a commercial electronic message that has an Australian link unless:

(a) the message clearly and accurately identifies the individual or organisation who authorised the sending of the message; and
(b) the message includes accurate information about how the recipient can readily contact that individual or organisation; and
(c) that information complies with the condition or conditions (if any) specified in the regulations; and
(d) that information is reasonably likely to be valid for at least 30 days after the message is sent.

(Commercial electronic messages must contain a functional unsubscribe facility) A person

must not send, or cause to be sent, a commercial electronic message unless the message includes:

(i) a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual or organisation who authorised the sending of the first mentioned message; or
(ii) a statement to similar effect; and the statement is presented in a clear and conspicuous manner; and

the electronic address is reasonably likely to be capable of receiving the recipient's unsubscribe message (if any); and a reasonable number of similar unsubscribe messages always sent by other recipients (if any) of the same message during a period of at least 30 days after the message is sent; and the electronic address is legitimately obtained.

(2) Labeling

In case of Australia, labeling obligation is not identified.

(3) Regulation on address harvesting software

The Spam Act prohibits the supply, acquisition or use of address-harvesting software and the use of lists generated by such software to transmit commercial electronic messages.

(Address-harvesting software and harvested-address lists must not be supplied) A person (the supplier) 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.

(Address-harvesting software and harvested-address lists must not be acquired) 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.

(Address-harvesting software and harvested-address lists must not be used) A person must not use address-harvesting software; or a harvested-address list.

3) Regulatory Authority

The Australia Communications and Media Authority (ACMA) is the sole enforcement agency

of the Spam Act. The authority has a wide range of enforcement mechanisms, from encouraging the development of industry codes to litigation seeking the recovery of losses or profits. Private companies and individuals can file a claim for damages once the ACMA has taken action in federal court and the court finds that there has been a violation.

The ACMA cooperates with other regulatory agencies in Australia. Predominantly this would include information sharing where jurisdiction of another regulatory agency is also triggered. Most commonly, this occurs between the ACMA and regulators responsible for consumer law, finance protections, or privacy law.

The ACMA does not collect demographic information (e.g., the population at large, children, elderly people, families, local communities, small businesses, local authorities, etc.) as part of spam complaints because collecting this information would likely contravene Australian privacy laws.

4) Penalties

Fines for individuals can be up to AUD 84,000 per day for the first offense and AUD 420,000 per day for the repeated offenses. In the case of a corporation, AUD 420,000 for the first offense and AUD 2.1 million for the repeated offenses can be imposed (which are the standard for penalty before 1 July 2020). No provision of the Spam Act imposes criminal liability for violations.

However, Australia does not have different penalties based on the subject of the message (e.g. financial services vs gambling). Penalties can take the form of infringement notices issued by the ACMA, formal warnings, court enforceable undertaking, or actions in the courts including injunctions and court imposed financial penalties. The penalties do however vary depending on: (a) The legislative provision that has been breached; (b) The number of breaches on a single day; (c) Whether a financial penalty is given by the ACMA or by the courts. The ACMA and the courts also have discretion concerning the number of breaches to be included in any financial penalty.

D. Spam Policy (non-regulatory method, government-funded)

1) Technical response (spam detection, analysis, and response technology development)

While the ACMA understands that spam filtering is common practice among internet and/or email services providers, it does not have any detailed information on these activities. The predominant agency in Australia is the Australian Communications and Media Authority

(ACMA). However, telecommunications service providers and internet and/or email services providers also play a role through their commercial spam filtering products and services for their customers.

2) Self-regulation

In response to the Review of the Australian Communications and Media Authority (the ACMA Review) conducted by the Department of Communications and the Arts (DoCA), the ACMA has examined the potential for self-regulation of:

- commercial electronic messages under the Spam Act 2003
- the Do Not Call Register (DNCR) and responsibilities for the Do Not Call Register Act 2006 (DNCR Act) and related industry standards
- the Integrated Public Number Database (IPND).

ACMA have found that the unsolicited communications functions should not be referred to industry, and the ACMA should retain its ability to outsource the DNCR, as per current arrangements (findings 1–4). The findings rely on evidence that:

- there is ongoing consumer concern about the impact and harms involved, with consumers believing the government has a key role in their prevention
- there is limited industry support for deregulation
- there is no consensus about which industry group, if any, would take on oversight of self-regulation of the functions
- alignment between the public and commercial interests involved is not strong, with key stakeholders and ACMA compliance activities indicating the alignment is not direct or extensive
- there is an ongoing need to underpin enforcement action with formal legal powers
- the international experience continues to indicate direct regulation is the preferred model across comparable jurisdictions (with the ability to outsource operations of do not call registers)

There is general support from industry and consumers for the continued government delivery of the functions. Further, the public and commercial interests do not align to the extent the functions should be devolved to industry. The direct regulatory model therefore remains appropriate.

3) Education/ Awareness raising

The ACMA, as the agency responsible for regulating spam in Australia, has an ongoing role in

relation to education activities. The ACMA provides education to both industry and consumers on its website www.acma.gov.au and via direct contact with peak bodies (advocacy groups or associations) and industry participants. This includes general information about the spam rules, and information on the ACMA's compliance and enforcement actions.

E. International Cooperation

Under section 42 of the Spam Act 2003, the ACMA's functions include to liaise with regulatory and other relevant bodies overseas about cooperative arrangements for the prohibition or regulation of unsolicited commercial electronic messages and/or address-harvesting software. 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). The ACMA has also helped establish, and has been an active contributor to, international forums such as the London Action Plan (LAP) (which later became known as the Unsolicited Communications Enforcement Network (UCENet)). UCENet brings together regulators, law enforcement and industry representatives from some 27 countries to address spam related issues under its MOU. The ACMA also has MoUs with both the USA and Canada which specifically address information sharing and collaboration on spam issues. In addition, Australia signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.1.2. Bhutan

A. Definition of spam

There are no general laws or regulations regarding spam, but The Bhutan Information and Communications and Media Act (ICM Act) 2018 has a clause on Unsolicited e-mail with the following details:

Unsolicited e-mail

347. An e-mail message which an ICT and Media facility or service provider or vendor may send shall prominently display a return e-mail address and shall provide in plain language, a simple procedure by which users or consumers can notify the concerned ICT and Media facility or service provider or vendor that they do not wish to receive such messages in the future.

B. Current status for spam response

Bhutan didn't provide the information related to how they identify and measure spam, how

they categorize the types of spam, and the volume of spam traffic in Bhutan. They have current challenges related to spam such as legislation, technical issues, and international cooperation. They don't have any legislation specific to spam, and source of spam is majorly from companies outside the country which cannot be regulated.

The government of Bhutan doesn't identify or measure spam by types of contents (e.g., gambling, loan, medicine, financial product, etc.) in the operational environment. They don't have 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 Bhutan, the government and telecommunication service providers are mainly engaged in anti-spam activities. However, government doesn't have any information on the anti-spam activities that the private sectors are currently doing. They don't categorize spam by its target (e.g., the population at large, children, elderly people, families, local communities, small businesses, local authorities, etc.). The Ministry of Information and Communication, Bhutan oversees spam related issues.

C. Legislation related to spam

Bhutan doesn't have general anti-spam act and any plan to legislate one because they have never experienced serious spam related issues, so they don't have any need to enact general anti-spam act. However, the Bhutan ICM Act 2018 has a clause on Unsolicited e-mail with the following details:

Chapter 17 "Protection of Online or Offline Privacy"

Unsolicited e-mail

347. An e-mail message which an ICT and Media facility or service provider or vendor may send shall prominently display a return e-mail address and shall provide in plain language, a simple procedure by which users or consumers can notify the concerned ICT and Media facility or service provider or vendor that they do not wish to receive such messages in the future.

In this act, they adopted the "Opt-out" scheme for the spam email. The senders should (1) display a return e-mail address and (2) should provide an unsubscribe facility (a simple procedure by which users can notify the senders that they do not wish to receive such messages in the future). However, Bhutan didn't provide any information on the regulation of spam messages and spam calls.

D. Spam policy

1) Technical response

The government of Bhutan doesn’t have any technical measures to prevent spam.

2) Self-regulation

There is no anti-spam self-regulation scheme in Bhutan.

3) Education/ Awareness raising

There is no anti-spam policy related to the education and awareness-raising on spam in Bhutan.

E. International cooperation

Bhutan doesn’t participate in any international cooperation initiatives on spam. They don’t have any plan to participate any international cooperation initiatives or create new one.

3.1.3. Brunei Darussalam

A. Definition of spam

Brunei doesn't have national law or regulation on spam related but generally spam is known as mass sending of unsolicited messages to mailing lists, individuals, organizations etc. for example, Internet emails or mobile short messaging service (SMS).

B. Current status for spam response

In Brunei, common types of spam identified are e-mail spam, SMS spam and spam in IP-based application. However, Brunei has no reporting system or mechanism for measuring spam traffic in Brunei and there is no unified approach to the issue of spam in Brunei.

Brunei has the current challenges related to spam on the legislation, technical issue, law enforcement and international cooperation. In detail, (1) Identity theft and fraud; Issue of renting out private line numbers or bank account details for gambling and criminal activities, (2) Consumer harm; Consumers are vulnerable to fraud, harassment, and misinformation, (3) Invasion of privacy; It is concerned about children’s exposure to spam and inappropriate content.

The government of Brunei identifies advertising the gambling related activities and loan related

activities through Short Message Services (SMS), social media platforms like Facebook and messaging application such as WhatsApp, WeChat, and Telegram.

In Brunei, the government and telecommunication service providers are mainly engaged in anti-spam activities. The telecommunication Service Providers have cooperated with the government authority and law enforcement agency in providing technical assistance and public awareness. Network operator, internet service providers, telecommunication companies are to cooperate with the government authority focusing on spam activities that are fraudulent or have the potential to cause harm, to monitor spam related activities and to provide access for consumer complaint. The national focal point is the Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) that facilitates complaints for spam activities via SMS.

C. Legislation related to spam

There is no general anti-spam act and no plan to legislate general anti-spam act because of lack of resources (information, experts, funds, etc.) and because they have never experienced serious spam related issues, so they don't have any need to enact general anti-spam act.

D. Spam policy

1) Technical response

Brunei network operator is expected to provide technical measures to prevent spam. From the government side, Brunei implemented no anti-spam technical solutions. And, Brunei doesn't have a plan to implement technical solutions from government side because of lack of resources (information, experts, funds, etc.).

2) Self-regulation

There is no anti-spam self-regulation scheme in Brunei. And, Brunei doesn't have a plan to create self-regulation scheme because of lack of resources (information, experts, funds, etc.) and not enough data to assess the extent of the problem.

3) Education/ Awareness raising

There is no specific anti-spam policy related to the education and awareness-raising on spam in Brunei. And, Brunei doesn't have any plan to create education and awareness-raising policy because they have general online safety awareness program which include issues related to

spam and it is conducted in a yearly basis. The Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) is in charge of this program. To ensure the safe use of the telecommunication services, AITI has conducted continuous initiatives in raising awareness of the public on general online safety including:

- Issue advisories and press releases related to spam messages
- Provide online safety learning materials for the school
- Produce and publish videos, audios and awareness materials for broadcast on television, radio and social media platforms
- Conduct awareness talks at schools and other learning institutions

Also, in Brunei there are private sector initiatives related to the education and awareness-raising on spam. The Brunei CERT is conducting these initiatives. They provide an awareness program called "Secure Verify Connect", aimed at raising awareness of Internet safety and information security among the public, though education, seminars, and workshops. "Secure Verify Connect" is an initiative by BruCERT aimed at increasing the awareness of Internet safety and information security among the Bruneian public. All have a responsibility to educate themselves about cyber threats and risks to privacy and safety. Children are especially vulnerable and need guidance so they can enjoy using the Internet safely.

E. International cooperation

Brunei doesn't participate in any international cooperation initiatives on spam. They don't have any plan to participate any international cooperation initiatives or create new one because of lack of resources (information, experts, funds, etc.) and not enough data to assess the extent of the problem. However, Brunei signed the Regional Comprehensive Economic Partnership (RCEP) agreement, and combating spam related to online gambling is dealt with by the law enforcement agency through their coordination mechanism.

Even though Brunei doesn't have any special activities related to the international cooperation on spam issues, when they counter spam effectively cross-border, they see the challenges of lack of technical resources and lack of buy-in from the relevant private sector agencies.

3.1.4. Cambodia

A. Definition of spam

In case of Cambodia, they don't have any definition of spam on regulation. However, they

recognize email spam, SMS spam, voice call spam and instant messenger spam.

B. Current status for spam response

In Cambodia, government doesn't have statistics regarding spam, and they aren't measuring spam from the government side.

In the case of Cambodia, survey result shows that there are issues related to the legislation, government-private sector cooperation, international cooperation regarding spam.

Therefore, when APT provides programs to enhance the capacity of member countries, Cambodia responded that programs such as training to government officials is needed. In the case of training, 1) an overall overview of the anti-spam legal system, 2) global norms and trends, 3) specific rules and regulations, 4) analysis of current regulations and problems of each APT member country, 5) best practices, recent development, etc., are particularly necessary. And Cambodia answered that the main target of the training should be the director general, director, deputy director and manager level government officers in charge of spam-related issues.

C. Legislation related to spam

1) Key concepts

There is no comprehensive anti-spam legislation in Cambodia. So, they don't have any definition of spam on regulation.

2) Contents of spam legislation

There is no comprehensive anti-spam legislation in Cambodia and currently they don't have any plan to legislate new act. However, Cambodian administration considers it is a little needed to legislate an act for spam prevention. They answered that they don't have any plan to legislate an act because of the lack of resources (information, experts, fund, etc.). Also, they don't feel any need because they have never experienced serious spam related issues.

3) Regulatory authority

Ministry of Post and Telecommunications (MPTC) is in charge of spam, but they don't have any cooperation with organization related to the type of advertisement.

4) Penalties

There is no comprehensive anti-spam legislation in Cambodia. So, they don't have any regulation on spam penalties.

4. Spam policy

1) Technical response

In the case of Cambodia, they have implemented technical solution, MaxBIT spam filter, which is provided by the Internet service provider, to prevent spam.

2) Self-regulation

Cambodia doesn't have anti-spam self-regulation scheme and survey shows that it is because of the lack of resources (information, experts, fund, etc.). Also, they don't feel any need because they have never experienced serious spam related issues. However, they answered that they expect the network operator to share information and best practice of monitoring and countering spam.

3) Education/ Awareness raising

At present, Cambodia doesn't have any education/ awareness raising programs and survey shows that it is because of the lack of resources (information, experts, fund, etc.). Also, they don't feel any need because they have never experienced serious spam related issues.

E. International cooperation

According to the survey, Cambodia hasn't joined any international cooperation initiatives and survey shows that it is because of the lack of resources (information, experts, fund, etc.). Also, they don't feel any need because they have never experienced serious spam related issues. However, they answered that they think sharing information and best practice of monitoring and countering spam as the challenges to counter spam effectively cross-border.

3.1.5. People's Republic of China

A. Definition of spam

In China, the definition of spam is as follows:

“Unsolicited Advertising, electronic publications, various forms of promotional materials and other promotional emails；The email can’t be rejected by the recipient；Hidden the sender’s identity, address, title; The email contain faked information sources, senders and routings”.

B. Current status for spam response

China identifies spam by the types of spam, for example, E-mail spam, SMS/MMS spam, spam in IP-based application (SNS, instant messenger, bulletin board), voice call spam, etc.

China also identifies and measures spam by types of contents (e.g., financial product, Health care, Leisure and entertainment, Loan).

The government of Chinas thinks the current challenges related to spam in China are legislation, technical issue, government-private sector cooperation, law enforcement, and international cooperation.

In China, government, telecommunication service providers, industry associations, and non-governmental organizations are all engaged in anti-spam activities. Especially, ISOC China (Internet Society of China) plays very important role in dealing with the issue of spam.

C. Legislation related to spam

Since the Internet and its application acquire rapid development, a series of problems related to Internet, for example the spam, have accompanied, which may lead to a lot of troubles. The flooding of spam will result in a mass of network resources being wasted, and the normal email corresponding being affected. Usually, spam is utilized by some network virus and hackers as a carrier for virus spreading, which has caused network security cases. It not only directly threatens the Internet information security, but also aggrieves email users' legitimate rights and corporation's benefits.

On these regards, in order to regulate Internet Email Services and safeguard the legal rights of the end users, Ministry of Information Industry (MII) of P. R. China enacted the first national anti-Spam regulation on March 30th, 2006, which is hereby formulated in accordance with related national laws on telecommunications and Internet.

On 20 February 2006 the Chinese Ministry of Information Industry (MII) of P. R. China adopted the Regulation for the Administration of Internet email Services, which took effect on 30 March 2006.

The legislation aims to regulate Internet email services and to protect end-users.

1) Key concepts

The definition of spam is:

Unsolicited Advertising, electronic publications, various forms of promotional materials and other promotional emails；The email can't be rejected by the recipient；Hidden the sender's identity, address, title; The email contain faked information sources, senders, and routings.

The term "Internet e-mail services" as mentioned in the present regulation shall refer to the activities of establishing Internet e-mail servers to provide conditions for Internet users to send and receive Internet e-mails.

2) Contents of spam legislation

(1) Regulatory framework

Basically, the Chinese government has an opt-in system for spam emails. Regulations on spam messages (SMS/MMS) and spam calls are not identified.

Internet E-mail Service Regulation applies only to e-mail and does not apply to other types of electronic communications such as SMS, MMS messages and fax. This regulation not only contain provisions governing the sending of spam, but also contain provisions governing the conduct of Internet e-mail service providers. For example, email service providers have been required to take steps to strengthen protection against their email servers to prevent them from being used by spammers.

Articles 13 and 14 of the Regulation provide that no person or organization may send:

- Emails with hidden or forged address information
- Commercial emails without the recipient's explicit consent
- Commercial emails without "AD" or equivalent Chinese characters in the subject line

- Commercial emails after the recipient have opted out of receiving the same email
- Commercial emails that do not contain valid sender contact information, including an email address, so that recipients can notify the sender that they no longer want to receive commercial emails if they so wish.

(Acquiring consent) 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; or

(Accurate sender information) No organization or individual may have the following acts of sending Internet e-mails by itself/himself or upon entrustment: Intentionally concealing or forging Internet e-mail envelope information.

(Stop sending again after receiving refusal) Where an Internet e-mail recipient refuses to continue receiving Internet e-mails containing commercial advertisement contents after clearly consenting to such receipt, the Internet e-mail senders shall stop sending them, unless otherwise agreed upon between both parties.

(Unsubscribe facility) An Internet e-mail service sender shall, when sending Internet e-mails containing commercial advertisement contents, provide the recipients with the means of contact for refusing to continue receiving the said e-mails, including the sender's e-mail address, and shall guarantee that the means of contact it provides will be valid within 30 days.

(2) Labelling

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.

(3) Other regulation

(Registration of IP addresses of the email servers) The state practices registration-based administration to the IP addresses of the e-mail servers of Internet e-mail service providers. An

Internet e-mail service provider shall, 20 days prior to the opening of the e-mail server, register the IP address of the Internet e-mail server in the Ministry of Information Industry of the People's Republic of China or the communication administrative bureau of the involved province, autonomous region, or municipality directly under the Central Government (hereinafter referred to as "the communication administrative bureau").

Where an Internet e-mail service provider intends to modify its e-mail server IP address, it shall go through the modification procedures 30 days in advance.

(Recording obligation) An Internet e-mail service provider shall record the time of sending or receiving Internet e-mails it sends or receives via its e-mail server, the Internet e-mail addresses and IP addresses of the senders and recipients. The foregoing records shall be kept for 60 days and shall be provided to the relevant state organ at the time of lawful inquiry.

(4) Regulation on address harvesting software

Internet e-mail service regulations prohibit the sale, distribution, or exchange of e-mail addresses (1) collected using address harvesting software or other automated means, or (2) generated by dictionary attacks.

Article 12 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.

3) Regulatory authority

MIIT, China is in charge of spam issues. Regarding spams related to illegal loans, Ministry of Public Security is also involved in.

4) Penalties

In case of violating the provisions such as prohibition of the use of automatically harvested addresses, obtaining consent, labeling, unsubscribe facility, etc., MIIT and other lawful regulators may order the correction of such violations and impose a fine of up to 10,000 yuan

(RMB). These fines can increase to 30,000 yuan if the sender has obtained illegal income from the violation.

Article 24

Whoever violates Article 12, 13 or 14 of the present Measures shall be ordered by the Ministry of Information Industry or the communication administrative bureau upon its powers to make a correction, and be fined up to 10,000 Yuan, in addition; if there are any illegal proceeds, it shall be fined up to 30,000 Yuan, in addition.

D. Spam policy

1) Technical response

In case of China, technical response for spam prevention is not identified.

2) Self-regulation

In case of China, Self-regulation for spam prevention is not identified.

3) Education/ Awareness raising

China has anti-spam policy related to the education and awareness-raising on spam, however, APT didn’t receive any specific information on this from China.

E. International cooperation

China joined UCENet to cooperate internationally. Also, China signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.1.6. The Cook Islands

A. Definition of spam

According to SPAM Act 2008, spam is an unsolicited ‘commercial electronic message'. The term 'commercial electronic message' includes electronic messages (e-mails, SMS text

messages, instant messages, but excluding voice calls) that sell goods, services, land, or business opportunities, etc.

B. Current status for spam response

In case of the Cook Islands, government and telecommunication service providers are mainly engaged in anti-spam activities. Mostly, service providers have information regarding volume of spam, types of spam, etc.

In the Cook Islands, survey result shows that there are issues related to the legislation, technical aspect, government-private sector cooperation, law enforcement, and international cooperation regarding spam.

Therefore, when APT provides programs to enhance the capacity of member countries, the Cook Islands responded that programs such as training to government officials is needed. In the case of training, 1) an overall overview of the anti-spam legal system, 2) global norms and trends, 3) specific rules and regulations, 4) best practices, recent development, etc., and 5) interactive workshops on solutions are particularly necessary. And the Cook Islands answered that the main target of the training should be the director general, director, deputy director and manager level government officers in charge of spam-related issues.

In the case of policy consulting, they answered that they need interview with domestic experts and drafting amendment to current law from experts dispatched by APT the most.

C. Legislation related to spam

1) Key concepts

The term 'commercial electronic message' includes electronic messages (e-mails, SMS text messages, instant messages, but excluding voice calls) that sell goods, services, land, or business opportunities, etc.

(Commercial Electronic message)

A **commercial electronic message** is an electronic message, where, having regard to -

(a) The content of the message; and
(b) The way in which the message is presented; and
(c) 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 of the purposes, of the message is-

(d) To offer to supply goods or services; or
(e) To advertise or promote goods or services; or
(f) To advertise or promote a supplier, or prospective supplier, of goods or services; or
(g) To offer to supply an interest in land; or
(h) To advertise or promote an interest in land; or
(i) To advertise or promote a supplier, or prospective supplier, of land or an interest in land; or
(j) To offer to provide a business opportunity or investment opportunity; or
(k) To advertise or promote a business opportunity or investment opportunity; or
(l) To advertise or promote a provider, or prospective provider, of a business opportunity or investment opportunity; or
(m) To assist or enable a person, by a deception, to dishonestly obtain property belonging to another person; or
(n) To assist or enable a person, by a deception, to dishonestly obtain a financial advantage from another person; or
(o) To assist or enable a person to dishonestly obtain a gain from another person; or
(p) A purpose specified in the regulations.

(Cook Islands link)

A particular message may have a Cook Islands link if it originates in the Cook Islands, if the device used to access the message is within the Cook Islands, if the recipient is an organization doing business in the Cook Islands or if the message was sent to a non-existent electronic address, but it reasonably appears that the message was accessed using a device located in Cook Islands.

More specifically, a commercial electronic message has the **Cook Islands link** if, if only if -

(a) the message originates in the Cook Islands; or
(b) the individual or organization who sent the message, or authorized the sending of the message, is an individual who is physically present in the Cook Islands when the message is sent; or an organisation whose central management and control is in the Cook Islands when the message is sent; or
(c) the computer, server, or device that is used to access the message is located in the Cook Islands; or
(d) the relevant electronic account-holder is an individual who is physically present in the Cook Islands when the message is accessed; or an organisation that carries on business or activities in the Cook Islands when the message is accessed; or
(e) if the message cannot be delivered because the relevant electronic address does not exist, assuming that the electronic address existed, it is reasonably likely that

the message would have been accessed using a computer, server, or device located in the Cook Islands.

2) Contents of spam legislation

(1) Regulatory framework

Basically, the Cook Islands government has an opt-in system for spam emails and messages. The Cook Islands' SPAM Act 2008 has basically the same structure as Australia's Spam Act. The Act prohibits the sending of unsolicited commercial electronic messages containing Cook Islands links.

Key Points for Compliance of Spam Act 2008

- Commercial electronic messages should not be sent without the prior consent of the recipient.

- All commercial electronic messages must include accurate sender information about who authorized the sending of the message and how to contact that person.

- All commercial electronic messages must include an "unsubscribe facility" by which the recipient can (at no cost) notify the sender that he or she will not receive such messages in the future.

(Unsolicited commercial electronic messages must not be sent)

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.

(Commercial electronic messages must include accurate sender information)

A person must not send, or cause to be sent, a commercial electronic message that has a Cook Islands link unless the message clearly and accurately identifies the individual or organization who authorised the sending of the message; the message includes accurate information about how the recipient can readily contact that individual or organization.

(Commercial electronic messages must contain functional unsubscribe facility)

A person must not send, or cause to be sent, a commercial electronic message that has a Cook Islands link unless the message includes a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual or organization who authorised the sending of the first-mentioned message.

(Acquiring consent)

Consent requirements apply to all commercial electronic messages, whether new or existing contacts information. This means that senders of commercial electronic messages must also obtain consent from people who are currently in their existing e-marketing contacts list. The consent can be express consent or inferred from the conduct, etc.

SPAM Act 2008

Schedule 2

CONSENT

For the purpose of this Act, "consent" means (a) express consent; or (b) consent that can be inferred from the conduct and the business and other relationships of the individual or organization concerned.

(2) Regulation on address harvesting software

The Act also prohibits the supply, acquiring and use of harvested electronic address lists or electronic address harvesting software intended to send unsolicited commercial electronic messages in violation of the Act.

SPAM Act Part 3

Rules about Address-harvesting Software and Harvested Address Lists

17. Address-harvesting software and harvested-address lists not to be supplied –

(1) A person must not supply or offer to supply-

(a) address-harvesting software; or

(b) a right to use address-harvesting software; or

(c) a harvested-address list; or

(d) a right to use a harvested-address list.

18. Address-harvesting software and harvested-address lists not to be acquired –

(1) A person must not acquire-

(a) address-harvesting software; or

(b) a right to use address-harvesting software; or

(c) a harvested-address list; or

(d) a right to use a harvested-address list.

19. Address-harvesting software and harvested-address lists not to be used –

(1) A person must not use-

(a) address-harvesting software; or

(b) a harvested-address list,

If the person is –

(c) an individual who is physically present in the Cook Islands at the time of the use; or

(d) a body corporate or partnership that carries on business or activities in the Cook Islands at the time of the use.

3) Regulatory authority

Office of the Prime Minister is in charge of spam regulation in Cook Islands.

4) Penalties

The pecuniary penalties for the violation of this Act can be up to $ 200,000 for individuals and $ 1,000,000 for corporations.

The court may order a person (the perpetrator) to pay a pecuniary penalty to the government, if the court is satisfied that the perpetrator has contravened a civil penalty provision.

If the perpetrator is an individual, the court may order the perpetrator to pay a pecuniary penalty not exceeding $200,000 in respect of the violation.

If the perpetrator is an organisation, the court may order the perpetrator to pay a pecuniary penalty not exceeding $1,000,000 in respect of the violation.

SPAM Act

PART 4

CIVIL PENALTIES

20. Pecuniary penalties for contravention of civil penalty provisions – (1) If the Court is satisfied that a person has contravened a civil penalty provision, the Court may order the person to pay to the Government such pecuniary penalty, in respect of each contravention, as the Court determines to be appropriate.

21. Maximum penalties for contravention of civil penalty provisions – (1) The maximum penalty payable under section 20 (1) by a person in respect of a contravention of a civil penalty provision depends on –

(a) whether the person has a prior record in relation to the civil penalty provision; and

(b) whether the person is a body corporate; and

(c) whether the civil penalty provision is section 14 (1), (6) or (9).

(3) If a body corporate does not have a prior record in relation to a particular civil penalty provision –

(a) the penalty payable under subsection 20 (1) by the body corporate in respect of a contravention of the civil penalty provision must not exceed –

(i) if the civil penalty provision is section 14 (1), (6) or (9) - $10,000; or

(ii) in any other cases - $5,000; and

(b) if the Court finds that the body corporate has, on a particular day, committed 2 or more contraventions of the civil penalty provision – the total of the penalties payable under section 20 (1) by the body corporate in respect of those contraventions must not exceed –

(i) if the civil penalty provision is section 14 (1), (6) or (9) - $200,000; or

(ii) in any other cases - $100,000.

(4) If a person other than a body corporate does not have a prior record in relation to a particular civil penalty provision –

(a) the penalty payable under subsection 20 (1) by the person in respect of a contravention of the civil penalty provision must not exceed –

(i) if the civil penalty provision is section 14 (1), (6) or (9) - $2,000; or

(ii) in any other cases - $1,000; and

(b) if the Court finds that the person has, on a particular day, committed 2 or more contraventions of the civil penalty provision – the total of the penalties payable under section 20 (1) by the person in respect of those contraventions must not exceed –

(i) if the civil penalty provision is section 14 (1), (6) or (9) - $40,000; or

(ii) in any other cases - $20,000.

(5) If a body corporate has a prior record in relation to a particular civil penalty provision –

(a) the penalty payable under subsection 20 (1) by the body corporate in respect of a contravention of the civil penalty provision must not exceed –

(i) if the civil penalty provision is section 14 (1), (6) or (9) - $50,000; or

(ii) in any other cases - $25,000; and

(b) if the Court finds that the body corporate has, on a particular day, committed 2 or more contraventions of the civil penalty provision – the total of the penalties payable under section 20 (1) by the body corporate in respect of those contraventions must not exceed –

(i) if the civil penalty provision is section 14 (1), (6) or (9) - $1,000,000; or

(ii) in any other cases - $500,000.

(6) If a person other than a body corporate has a prior record in relation to a particular civil penalty provision –

(a) the penalty payable under subsection 20 (1) by the person in respect of a contravention of the civil penalty provision must not exceed –

(i) if the civil penalty provision is section 14 (1), (6) or (9) - $10,000; or

(ii) in any other cases - $5,000; and

(b) if the Court finds that the person has, on a particular day, committed 2 or more contraventions of the civil penalty provision – the total of the penalties payable under section 20 (1) by the person in respect of those contraventions must not exceed –

(i) if the civil penalty provision is section 14 (1), (6) or (9) - $200,000; or

(ii) in any other cases - $100,000.

Also, persons affected by the violation of the Act may seek an injunction from the Court or may apply to the Court for compensation or damages.

D. Spam policy

1) Technical response

In case of the Cook Islands, mainly the local telecommunication service provider (Vodafone Cook Islands) handles technical response for spam prevention. However, the details are not identified.

2) Self-regulation

In case of the Cook Islands, currently they don't have any self-regulation scheme for spam prevention and don't have any plan for it because they think working on cybersecurity can cover SPAM issue.

3) Education/ Awareness raising

In case of the Cook Islands, education and awareness raising activities for spam response is not identified.

E. International Cooperation

The Cook Islands didn't join the UCENet or the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.1.7. Hong Kong

A. Definition of spam

In Hong Kong, China, the Unsolicited Electronic Messages Ordinance (UEMO) regulates the sending of unsolicited commercial electronic messages (messages with a commercial purpose such as promoting a product or service or a service provider) with a Hong Kong link, irrespective of whether the messages might be harmful or deceptive, etc.

More specifically, commercial electronic message means an electronic message the purpose, or one of the purposes, of which is—

(a) to offer to supply goods, services, facilities, land or an interest in land;
(b) to offer to provide a business opportunity or an investment opportunity;
(c) to advertise or promote goods, services, facilities, land or an interest in land;
(d) to advertise or promote a business opportunity or an investment opportunity;

(e) to advertise or promote a supplier, or a prospective supplier, of goods, services, facilities, land or an interest in land; or
(f) to advertise or promote a provider, or a prospective provider, of a business opportunity or an investment opportunity,

in the course of or in the furtherance of any business.

B. Current status for spam response

Hong Kong identifies and measures spams by reports and complaints received from the public. Major types of spam include email messages, short messages (including SMS/MMS and short messages via instant messengers), pre-recorded voice call messages and fax messages.

The enforcement statistics of Unsolicited Electronic Messages Ordinance (UEMO) is as below table.

	No. of reports received						No. of reports dealt with	No. of warning letters issued	No. of enforcement notices issued	No. of Prosecutions instituted
	Fax	Email	Short Message	Pre-recorded Telephone Message	Others	Total				
10.2021	4	7	4	15	2	32	42	2	0	0
9. 2021	4	6	22	8	5	45	54	2	0	0
8. 2021	16	5	14	8	4	47	34	1	0	0
7. 2021	3	10	18	14	5	50	39	1	0	0
6. 2021	0	12	21	8	2	43	61	3	0	0
5. 2021	9	6	17	11	4	47	40	0	0	0
4. 2021	1	12	21	15	1	50	42	0	0	0
3.	3	9	10	18	2	42	53	1	0	0

2021										
2. 2021	0	8	10	6	2	26	61	1	0	0
1. 2021	2	13	24	12	1	52	37	1	0	0
12.2020	2	17	20	11	7	57	38	0	0	0
11.2020	4	10	14	17	4	49	64	0	0	0
Sub-total (12 mths)	48	115	195	143	39	540	565	12	0	0

	No. of reports received						No. of reports dealt with	No. of warning letters issued	No. of enforcement notices issued	No. of Prosecutions instituted
	Fax	Email	Short Message	Pre-recorded Telephone Message	Others	Total				
2021 (Oct)	42	88	161	115	28	434	463	12	0	0
2020	53	130	228	108	37	556	526	20	0	0
2019	55	118	330	62	57	622	630	31	0	0
2018	138	115	290	56	26	625	749	30	0	0
2017	202	185	155	207	51	800	1789	42	0	0
2016	208	177	204	142	60	791	855	26	0	1
2015	516	324	968	182	106	2096	1520	28	2	0
2014	383	400	772	223	120	1898	1748	52	1	1

2013	574	426	606	280	160	2046	2012	97	8	0
2012	809	567	464	688	101	2629	3364	66	6	0
2011	1350	356	168	613	111	2598	3019	109	7	0
2010	1774	436	262	532	101	3105	3308	174	1	0
2009	4413	804	308	363	194	6082	6766	93	1	0
2008	6127	1092	477	699	397	8792	6173	67	0	0
Total	16644	5218	5393	4270	1549	33074	32922	847	26	2

*"others" includes person-to-person commercial calls, silent calls, beep tone calls, etc.

* 2008 data is for the period from 22 December 2007 to 31 December 2008

In Hong Kong, the major challenges are the source of sender being untraceable, and the emerging use of artificial intelligence/chatbots in telemarketing activities, which increase difficulty and adds up complexity in the enforcement work.

Hong Kong doesn't identify or measure spam by types of contents (e.g., gambling, loan, medicine, financial product, etc.) in the operational environment. Also, the government of Hong Kong hasn't estimated how much spam incidents cost to the economy of the country or organization.

Mainly Government and Telecom service providers are engaged in anti-spam activities, and telecommunications service providers in general handle spam-related complaints for their customers.

C. Legislation related to spam

1) Key concepts

The Unsolicited Electronic Messages Ordinance (UEMO) was enacted on 23 May 2007 and came into full force on 22 December 2007.

(1) **commercial electronic message** means an electronic message the purpose, or one of the purposes, of which is—

(a) to offer to supply goods, services, facilities, land or an interest in land;
(b) to offer to provide a business opportunity or an investment opportunity;
(c) to advertise or promote goods, services, facilities, land or an interest in land;
(d) to advertise or promote a business opportunity or an investment opportunity;
(e) to advertise or promote a supplier, or a prospective supplier, of goods, services, facilities, land or an interest in land; or
(f) to advertise or promote a provider, or a prospective provider, of a business opportunity or an investment opportunity, in the course of or in the furtherance of any business;

electronic message (電子訊息) includes a message in any form sent over a public telecommunications service to an electronic address and includes, but is not limited to—

(a) a text, voice, sound, image or video message; and
(b) a message combining text, voice, sound, images or video;

(2) Meaning of **Hong Kong link**

(1) For the purposes of this Ordinance, a commercial electronic message has a Hong Kong link if, and only if—

(a) the message originates in Hong Kong;
(b) the individual or organization who sent the message or authorized the sending of the message is—
  (i) an individual who is physically present in Hong Kong when the message is sent;
  (ii) an organization (other than a Hong Kong company) that is carrying on business or activities in Hong Kong when the message is sent; or
  (iii) a Hong Kong company;
(c) the telecommunications device that is used to access the message is located in Hong Kong;
(d) the registered user of the electronic address to which the message is sent is—
  (i) an individual who is physically present in Hong Kong when the message is accessed; or
  (ii) an organization that is carrying on business or activities in Hong Kong when the message is accessed; or
(e) the message is sent to an electronic address that is allocated or assigned by the Authority.

(2) For the purposes of subsection (1)(b), (c), (d) and (e), it is immaterial whether the commercial electronic message originates in Hong Kong or elsewhere.

(3) For the purposes of subsection (1)(b)(iii), it is immaterial whether the commercial electronic message is sent, or is authorized to be sent, from Hong Kong or elsewhere.

2) Contents of spam legislation

(1) Regulatory framework

Basically, the Hong Kong government has an opt-out system for spam emails, messages, and phone calls.

Unsolicited electronic message ordinance of Hong Kong was enacted in May 2007. Most of the provisions of the ordinance came into force on June 1, 2007, with the exception of Part 2. Part 2 of the Act, dealing with sending, causing, or attempting to send unsolicited electronic messages, came into force on 22 December 2007. The Act governs all forms of electronic messages, including e-mail, fax, SMS, MMS, and voice and multimedia messages generated in an automated manner (e.g. messages sent through interactive voice response systems). It applies to messages with Hong Kong link, including those sent by or received by the recipient within Hong Kong, or where the sender was a Hong Kong company or organization doing business in Hong Kong at the time the message was sent.

The ordinance creates an opt-out mechanism for sending unsolicited commercial electronic messages. Commercial electronic messages are electronic messages sent for the purpose of offering or advertising goods, services, facilities, land or provision of land or, among other things, promoting or advertising business or investment opportunities. Part 2 does not apply to many other types of transactional messages and messages related to pre-existing relationship, including for the main purposes of the following:

- For the purpose of executing, completing or confirming previously agreed commercial transactions;
- To provide warranty, product recall, safety or security information for commercial products or services;
- For the purpose of delivery of goods or services, including product upgrades or updates, which are intended to be received by the recipient under the transaction;
- For the purpose of providing notice of account information related to products, changes in terms or features of products, or changes in recipient status
- For the purpose of providing information on the employment relationship related to the recipient or information about the relevant benefit plan;

In addition, the provisions of Part 2 do not apply if the message was sent by mistake or if people

were not aware or could not have known through reasonable efforts that the message contained a Hong Kong link.

Part 2 of the ordinance stipulates people cannot send commercial electronic messages if (1) the messages do not contain the accurate sender information, (2) they lack a functional unsubscribe facility, (3) they have an incorrect subject heading, and (4) telephone line identification information are concealed when messages are sent by phone or fax, (5) the unsubscribe request was sent to the designated email address 10 business days prior to the additional message being sent, and (6) the messages are sent to the address registered in the do-not-call register.

The opt-out request (or evidence of consent) must be retained by the regulated body for at least three years after receipt.

The Legislative Council also enacted regulations under Part 2 of the ordinance specifying how sender's contact information should be displayed and the types of unsubscribe facility that should be used. This regulation came into force at the same time that Part 2 of the ordinance came into force.

(Including accurate sender information) A person shall not send a commercial electronic message that has a Hong Kong link unless—

(a) the message includes clear and accurate information identifying the individual or organization who authorized the sending of the message;
(b) the message includes clear and accurate information about how the recipient can readily contact that individual or organization;
(c) the message includes such information and complies with such conditions as is or are specified in the regulations, if any; and
(d) the information included in the message in compliance with this subsection is reasonably likely to be valid for at least 30 days after the message is sent.

(Unsubscribe facility) A person shall not send a commercial electronic message that has a Hong Kong link unless—

(a) the message includes—
  (i) a statement to the effect that the recipient may use an electronic address or other electronic means specified in the message (the unsubscribe facility) to send an unsubscribe request to the individual or organization who authorized the sending of the message; or
  (ii) a statement to similar effect;
(b) the statement is presented in a clear and conspicuous manner;

(c) the statement complies with such conditions as are specified in the regulations, if any;
(d) the unsubscribe facility complies with such conditions as are specified in the regulations, if any;
(e) if the unsubscribe facility is a telephone number or facsimile number, it is a number allocated or assigned by the Authority;
(f) the unsubscribe facility is reasonably likely to be capable of receiving the recipient's unsubscribe request, if any, at all times during a period of at least 30 days after the message is sent; and

the unsubscribe request may be sent by the recipient free of any charge to the recipient for the use of the unsubscribe facility

(Commercial electronic messages must not be sent after unsubscribe request is sent)

The individual or organization shall, within 10 working days from the day on which the unsubscribe request is sent—

(a) cease sending any further commercial electronic messages to the electronic address in respect of which the unsubscribe request was sent; and
(b) cease authorizing the sending of any further commercial electronic messages to that electronic address.

(Do-not-call register) A person shall not send a commercial electronic message that has a Hong Kong link to an electronic address that, at the time the message is sent, is listed in a do-not-call register.

(2) Labeling

(Must not use misleading subject headings)

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

(3) Regulation on address harvesting software

The ordinance prohibits the supply of address-harvesting software and prohibits the supply of

harvested address lists in connection with the sending of commercial electronic messages. Violations of the ordinance also occur when obtaining or using address harvesting software, when obtaining or using the harvested address list, when obtaining the right to use the address harvesting software/harvested address list as well as sending electronic messages in an automated manner. All such violations are punishable by up to five years in prison and a fine of up to HKD 1 million.

(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;

3) Regulatory authority

Office of the Communications Authority (OFCA) is in charge of the spam related issues.

- Authority may approve codes of practice; establish do-not-call registers; issue directions to telecommunications service providers; impose financial penalties; obtain information or documents relevant to investigation; issue enforcement notice.
- Authority or an authorized officer may, without warrant, arrest any person whom the Authority or authorized officer reasonably suspects of having committed a specified offence
- Authority may have power of magistrate to issue search warrant

4) Penalties

When a telecommunications regulator suspects that a person has violated part 2 of the ordinance, the regulator may issue a notice with details of the alleged violation and specific actions the violator must take to address the non-compliance. Violators who fail to comply with this notice will be in violation of the ordinance and will be subject to a fine of up to HKD 500,000 in addition to a daily fine of up to HKD1,000 per day for the duration of the violation.

(Offence relating to enforcement notices) A person who contravenes an enforcement notice served on him commits an offence.

A person who commits an offence under this section is liable on a second or subsequent conviction, to a fine of $500,000, and, in the case of a continuing offence, to a further daily fine of $1,000 for each day during which the offence continues.

The most severe punishment under the ordinance can be occurred when (1) send a bulk message using a communication device accessed without permission; (2) send multiple messages with

the intent to deceive or mislead the recipient of the messages; (3) forge header information in multiple messages; (4) submit forged identity information to obtain electronic addresses and domain names and use these addresses and domain names to send multiple commercial electronic messages; (5) falsely represents the registrant of electronic address and domain name and sends multiple commercial electronic messages from these addresses or domain names. Those who commit these violations could face up to 10 years in prison or a fine (with no specified maximum amount).

(Initiating transmission of multiple commercial electronic messages from telecommunications device, etc., accessed without authorization)

A person who

(a) accesses a telecommunications device, service, or network without authorization; and
(b) knowingly initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from that telecommunications device, service, or network,

commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(Initiating transmission of multiple commercial electronic messages with intent to deceive or mislead recipients as to source of messages) A person who knowingly initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from a telecommunications device, service or network without authorization, with the intent to deceive or mislead recipients as to the source of such messages, commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(Falsifying header information in multiple commercial electronic messages) A person who—

(a) materially falsifies header information in multiple commercial electronic messages that have a Hong Kong link; and
(b) knowingly initiates the transmission of such messages from a telecommunications device, service, or network,

commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(Registering for electronic addresses or domain names using information that falsifies identity of actual registrant) (1)A person who (a)registers, using information that materially

falsifies the identity of the actual registrant, for 5 or more electronic addresses or 2 or more domain names; and (b)knowingly initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from any of such electronic addresses or domain names or from any combination of such electronic addresses or domain names, commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

(False representations regarding registrant or successor in interest to registrant of electronic address or domain name) A person who (a)falsely represents himself to be the registrant or the legitimate successor in interest to the registrant of 5 or more electronic addresses or 2 or more domain names; and (b)knowingly initiates the transmission of multiple commercial electronic messages that have a Hong Kong link from any of such electronic addresses or domain names or from any combination of such electronic addresses or domain names, commits an offence and is liable on conviction on indictment to a fine and to imprisonment for 10 years.

D. Spam policy

1) Technical response

The Communications Authority established three Do-not-call (DNC) Registers, for fax, short messages, and pre-recorded telephone messages. The DNC Registers were established in about December 2007.

By Aug 2021, over 2.69 million telephone numbers were registered with the three DNC registers. Also, the number of unsolicited electronic messages complaint cases keeps on declining in the last three-year period.

2) Self-regulation

Hong Kong has anti-spam self-regulation scheme. The telecommunications, finance, and insurance sectors as well as call centers in Hong Kong have adopted the self-regulatory scheme on P2P marketing calls. Companies participating in the voluntary scheme should observe the requirements set out therein.

- For telecommunications sector, The Communications Association of Hong Kong;
- For finance sector, The Hong Kong Association of Banks and the Hong Kong Association of Restricted License Banks and Deposit-taking Companies;
- For insurance sector, The Hong Kong Federation of Insurers;
- For call centers, The Hong Kong Call Centre Association;

are the administrative institutions that are in charge of these self-regulation schemes.

(1) Telecommunications Sector

Telecommunications sector has "Code of Practice on Person-to-Person Marketing Calls"

Hours of Calling

Person-to-person marketing calls should only be made between Hong Kong time 9:00am and 10:00pm, unless the called party has advised that a call at another time would be more convenient and acceptable.

Identity and Purpose

A telemarketer who makes a person-to-person marketing call should not conceal or withhold from the called party the calling line identification information of the sending telephone number, or issue any instruction in connection with making the call that has the same effect

At the commencement of a person-to-person marketing call, the following information should be provided to the called party:

(a) the name of the principal that authorized the making of the call; and

(b) the purposes of the call.

Upon request, the called party should be informed of a telephone number of the telemarketer ("Contact Telephone Number") which he can call during normal business hours to lodge complaints against the person-to-person marketing calls made by staff or to make enquiries with staff.

Unsubscribe Request

A telemarketer should not make any further person-to-person marketing calls to a number after the registered user of that number has made an unsubscribe request to him or his principal within 10 working days in accordance with UEMO principles unless with the explicit consent form the registered user.

A telemarketer should accept an unsubscribe request made during a person-to-person marketing call, as well as an unsubscribe request made when a person calls at the Contact Telephone Number as mentioned in paragraph 9 above. A telemarketer may choose to offer

other additional channels for members of the public to make an unsubscribe request.

A telemarketer should and his principal should ensure that the list of telephone numbers in respect of which unsubscribe requests have been made should be properly maintained and updated within 10 working days in accordance with UEMO principle, and that telemarketers should not make person-to-person marketing calls to the telephone numbers on the up-to-date list.

Statistics of Complaints

A telemarketer and a principal should keep a proper record of statistics of complaints in relation to person-to-person marketing calls and provide statistics of complaints to the Association and the relevant authority or public body from time to time as requested by the Association and the relevant authority or public body for the purpose of monitoring the compliance situation.

Use of Automated Dialing Equipment

Telemarketers using automated dialing equipment should allow at least 15 seconds or four rings before disconnecting an unanswered call.

The called party should be connected to a live agent within two seconds after the call has been answered. Otherwise, the call is considered abandoned whether the call is eventually connected. Telemarketers should frequently review the percentage of abandoned calls and make every endeavor to minimize such percentage which shall not be greater than 10% of the total calls.

The automated dialing equipment deployed should be capable of generating relevant statistics for monitoring and ensuring compliance with this Code of Practice.

Called Party Who is Travelling Overseas when the Call is Made

If a telemarketer, when making a person-to-person marketing call, is aware that the called party is travelling overseas, he/she should endeavor to disconnect the call immediately (if the call has not yet been answered by the called party) or terminate the conversation as soon as practicable (if the call has been answered by the called party).

(2) Finance Sector

Finance sector has “Code of Practice on Person-to-Person Marketing Calls”.

Hours of Calling

Generally, person-to-person marketing calls should only be made between Hong Kong time 9:00am and 10:00pm, unless the called party has advised that a call at another time would be more convenient and acceptable or a call outside this period is allowed under the guidelines published in accordance with the Banking Ordinance (Cap.155), the Supervisory Policy Manual of the Hong Kong Monetary Authority ("HKMA") or other regulatory requirements applicable to Ais.

Identity and Purpose

A telemarketer who makes a person-to-person marketing call should not purposely conceal or withhold from the called party the calling line identification information of the sending telephone number or issue any instruction in connection with making the call that has the same effect.

(a) Subject to subsection (b), at the commencement of a person-to-person marketing call, the telemarketer should address the called party by his full name and provide the following information to the called party:

(i) the telemarketer's full name;

(ii) the name of the principal that authorized the making of the call;

(iii) the purposes of the call; and

(iv) an official telephone number of the principal ("Contact Telephone Number") which he can call during normal business hours to verify the identity of the telemarketer, lodge complaints in respect of the person-to-person marketing calls made or authorized to be made by the principal or to make enquiries with the principal.

(b) Subsection (a) does not apply to a relationship / account manager making marketing calls to his / her designated client(s) with whom he / she has already established a business relationship, as part of his /her duty to provide service to these client(s).

Unsubscribe Request

A telemarketer should not make any further person-to-person marketing calls to an individual, be it prospective or existing customer, after the individual has made an unsubscribe request to him or to his principal (refer to paragraph 12).

A telemarketer should accept an unsubscribe request made during a person-to-person

marketing call, as well as an unsubscribe request made when a person calls at the Contact Telephone Number as mentioned in paragraph 9 above. A telemarketer may choose to offer other additional channels for the called party of the public to make an unsubscribe request.

A telemarketer and a principal should ensure that the unsubscribe list is properly maintained and updated regularly; in the case of lists maintained and distributed on a computer network, this should be done as soon as the unsubscribe request is received and in other cases updates should be circulated to telemarketers at least once per week.

An individual may make a request to a telemarketer to delete him / her from the unsubscribe list. A telemarketer, however, should not initiate contact with the individuals on the unsubscribe list within the first two years after the individuals have first been included in the unsubscribe list to ascertain whether they would like to start to receiving person-to-person

marketing calls.

Further Collection of Information

If information is to be collected from the called party subsequent to the person-to-person marketing call, the telemarketer should provide to the called party for the purposes of sending such information the contact information of the principal or the telemarketer which is publicized by the principal (e.g., on the principal's website) and can be verified by the called party. Where the marketing call is made by a relationship / account manager to his / her own designated client(s) with whom he / she has already established a relationship, as part of his / her duty of serving the client(s), he / she needs only to provide the contact information of the principal upon request of the called party.

Subsequent Meetings

If any meeting is to be held with the called party subsequent to the person-to-person marketing call, the called party should be advised to visit the premises of the principal or the telemarketer which are publicized by the principal (e.g., on the principal's website) or contact the principal via the official channels to arrange the meeting to be held at any other places. For the purposes of this clause, a relationship / account manager making marketing calls to his / her own designated client(s) with whom he / she has already established a relationship, as part of his / her duty of serving the client(s), may agree with the called party on the venue of the meeting which may be outside the principal's premises.

Complaints

A telemarketer and a principal should keep a proper record of complaints in relation to person-

to-person marketing calls, and provide statistics of complaints to the HKMA, the Office of the Privacy Commissioner for Personal Data and the Commerce and Economic Development Bureau upon request.

Use of Automated Dialing Equipment

Telemarketers using automated dialing equipment should allow at least 5 seconds or four rings before disconnecting an unanswered call.

Calls using automated dialing equipment which are disconnected by the called party ultimately due to non-connection to a live agent after the call has been answered are considered as abandoned calls. Telemarketers should frequently review the percentage of abandoned calls and make every endeavor to minimize such percentage.

The automated dialing equipment deployed should be capable of generating relevant statistics for monitoring and ensuring compliance with this Code of Practice.

Called Party Who is Travelling Overseas when the Call is Made

If a telemarketer, when making a person-to-person marketing call, is aware that the called party is travelling overseas, he should endeavor to disconnect the call immediately (if the call has not yet been answered by the called party) or terminate the conversation as soon as practicable (if the call has been answered by the called party) unless prior consent has been obtained.

Relationship/Account Managers

A relationship / account manager should observe the requirements of this CoP when making person-to-person marketing calls except otherwise stated in sections 9, 14 and 15 when he / she makes marketing calls to his/her own designated client(s), with whom he/she has already established a relationship, as part of his / her duty of serving the client(s).

(3) Insurance Sector

Insurance sector has “Code of Practice on Person-to-Person Marketing Calls”.

Hours and Day of Calling

Person-to-person marketing calls should only be made between Hong Kong time 9:00 am and

10:00 pm, unless the called party has advised that a call at another time would be more convenient and acceptable or a call outside this period is allowed under the guidelines published in accordance with the Banking Ordinance.

Calls should be avoided on Sundays and public holidays, unless the telemarketer has grounds to believe that the calls will be readily acceptable.

Identity, Purpose, and Consent

A telemarketer who makes a person-to-person marketing call should not conceal or withhold from the called party the calling line identification information of the sending telephone number or issue any instruction in connection with making the call that has the same effect.

Taping of telephone conversations may be used to record the selling process of insurance products/services or any other financial services or for training purposes and quality control. Called party who expresses interest in the products should be advised when a call is to be recorded for such purpose. Recorded calls may not be disclosed to any third party without the consent of both parties to the call, except it is required by the law to disclose.

At the commencement of a person-to-person marketing call, the following information should be provided to the called party:

- the name of the principal that authorized the making of the call
- the name of the insurer, in the case where the person-to-person marketing call is authorized by the principal who is the insurance agent or the insurance agency and
- the purpose of the call

As far as practicable upon the called party's request, the called party should be informed of a telephone number ("Contact Telephone Number") which he can call during normal business hours to lodge complaints in respect of the person-to-person marketing calls made or authorized to be made by the principal or to make enquiries with the principal.

Unsubscribe Request

A principal should, as soon as practically possible, not make or authorize to make any further person-to-person marketing calls to a number after the registered user of that number has made an unsubscribe request to the principal or to a telemarketer, unless with explicit consent from the registered user.

A principal/telemarketer may ask the called party if he wishes to make an unsubscribe request during a person-to-person marketing call or accept an unsubscribe request made when a person calls at the Contact Telephone Number as mentioned above. A principal/telemarketer may choose to offer other additional channels for members of the public to make an unsubscribe

request.

A principal should ensure that the list of telephone numbers in respect of which unsubscribe requests have been made should be properly maintained and updated as soon as practicable, and that all telemarketers should not make person-to-person marketing calls to the telephone numbers on the up-to-date list.

Statistics of Complaints

A telemarketer and a principal should keep a proper record of statistics of complaints in relation to person-to-person marketing calls and provide statistics of complaints to the HKFI (Hong Kong Federation of Insurers) and the Insurance Authority or public body from time to time as requested by the HKFI and the Insurance Authority or public body for the purpose of monitoring the compliance situation.

Use of Automated Dialing Equipment

Telemarketers using automated dialing equipment should allow 15 seconds or four rings before disconnecting an unanswered call.

The called party should be connected to a live agent within two seconds after the call has been answered. The principal should keep track of the abandoned call ratio and maintain the level of such ration to below 10%.

The automated dialing equipment deployed should be capable of generating relevant statistics for monitoring and ensuring compliance with this Code of Practice.

Called party who is travelling overseas when the call is made

If a telemarketer, when making a person-to-person marketing call, is aware that the called party is travelling overseas, he/she should endeavor to disconnect the call immediately (if the call has not yet been answered by the called party) or terminate the conversation as soon as possible (if the call has been answered by the called party).

Conduct of telemarketer

The telemarketer shall;

- not engage in conduct, which is considered misleading, deceptive and harassing to customers. Statements which are untrue, fraudulent, or unjustly disparaging of competitors must not be used

- not conduct the offer or solicitation in the guise of research or survey when the real purpose is to sell
- terminate the call if a request to terminate the conversation is made by the called party
- accept the unsubscribe request and take appropriate and timely action not to make any further person-to-person marketing calls
- give proper introduction of the insurer he/she is acting for when making the calls and the purpose of the call state clearly the product features, premium and charges, the terms and conditions
- when finalizing any agreement, state clearly the total cost, relevant terms and conditions and payment plans, plus the amount or existence of any charges (if applicable) such as handling fees. These terms must be confirmed in writing if requested
- read back to the called party all relevant details of the credit card and must be satisfied that the called party understands that the transaction will be charged to the credit if the called party agrees to buy the product with the telemarketer and authorizes the charge to be made on a credit card and supplies relevant details over the phone and
- provide a contact number of the insurer to call for inquiries and complaints after a customer agrees to buy a product.

Post-sale

Copies of all relevant documents, agreements, contracts and/or statements of legal rights must be sent promptly to the called party.

(4) Call centers

Call centers have “Code of Practice on Person-to-Person Marketing Calls”.

Hours of Calling

Person-to-person marketing calls should only be made between Hong Kong time 9:00am and 10:00pm, unless the called party has advised that a call at another time would be more convenient and acceptable or a call outside this period is allowed under the guidelines published in accordance with the Banking Ordinance (Cap.155).

Identity and Purpose

A telemarketer who makes a person-to-person marketing call should not conceal or withhold from the called party the calling line identification information of the sending telephone

number or issue any instruction in connection with making the call that has the same effect.

At the commencement of a person-to-person marketing call, the following information should be provided to the called party:

(a) the name of the principal that authorized the making of the call; and

(b) the purposes of the call.

As far as practicable, the called party should be informed of a telephone number ("Contact Telephone Number") which he can call during normal business hours to lodge complaints in respect of the person-to-person marketing calls made or authorized to be made by the principal or to make enquiries with the principal.

Unsubscribe Request

(For use by associations)

A principal should not make or authorize to make any further person-to-person marketing calls to a number after the registered user of that number has made an unsubscribe request to the principal or to a telemarketer. OR

(For use by individuals or organizations)

A telemarketer should not make any further person-to-person marketing calls to a number after the registered user of that number has made an unsubscribe request to him or to his principal.

A telemarketer should accept an unsubscribe request made during a person-to-person marketing call, as well as an unsubscribe request made when a person calls at the Contact Telephone Number as mentioned in paragraph 10 above. A telemarketer may choose to offer other additional channels for members of the public to make an unsubscribe request.

A telemarketer and a principal should ensure that the list of telephone numbers in respect of which unsubscribe requests have been made should be properly maintained and updated as soon as practicable, and that all telemarketers should not make person-to-person marketing calls to the telephone numbers on the up-to-date list.

Statistics of Complaints

A telemarketer and a principal should keep a proper record of statistics of complaints in relation to person-to-person marketing calls and provide statistics of complaints to Hong Kong Call Centre Association and the relevant authority or public body from time to time as requested by the association and the relevant authority or public body for the purpose of monitoring the compliance situation.

Use of Automated Dialing Equipment

Telemarketers using automated dialing equipment should allow 15 seconds or four rings before disconnecting an unanswered call.

The called party should be connected to a live agent within two seconds after the call has been answered. The maximum percentage of abandoned calls should be 5%. Telemarketers should frequently review the percentage of abandoned calls and make every endeavor to minimize such percentage.

The automated dialing equipment deployed should be capable of generating relevant statistics for monitoring and ensuring compliance with this Code of Practice.

Called Party Who is Travelling Overseas when the Call is Made

If a telemarketer, when making a person-to-person marketing call, is aware that the called party is travelling overseas, he/she should endeavor to disconnect the call immediately (if the call has not yet been answered by the called party) or terminate the conversation as soon as practicable (if the call has been answered by the called party).

3) Education/ Awareness raising

The anti-spam response scheme of Hong Kong is quite well organized, Hong Kong has anti-spam policy related to the education and awareness-raising on spam. The government has been organizing education and publicity programmes to educate the public on the anti-spam matters.

From September 2018 to August 2021, the Office of the Communications Authority organized eight public seminars and eight roving exhibitions to promote proper use of various communications services.

These initiatives are considered as effective given that the number of unsolicited electronic messages complaint cases keep on declining in the last three-year period.

E. International Cooperation

Trade and Industry Department of the Hong Kong SAR Government is responsible to strengthen international co-operation initiatives on spam in the context of “electronic commerce”. For examples, there are “Free Trade Agreement between Hong Kong, China, and Australia (Chapter 11, Article 11.11 on Unsolicited Commercial Electronic Messages)” and “Regional Comprehensive Economic Partnership Agreement (RCEP) (Chapter 12, Article 12.9 on Unsolicited Commercial Electronic Messages)”.

Free Trade Agreement between Hong Kong, China, and Australia (Chapter 11, Article 11.11 on Unsolicited Commercial Electronic Messages)

Article 11.11: Unsolicited Commercial Electronic Messages

1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that:

> (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of such messages; or
>
> (b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages.

2. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages who do not comply with that Party's measures implemented pursuant

to paragraph 1.

3. The Parties shall endeavor to cooperate in cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

Regional Comprehensive Economic Partnership Agreement (RCEP) (Chapter 12, Article 12.9 on Unsolicited Commercial Electronic Messages)

Article 12.9: Unsolicited Commercial Electronic Messages

1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that:

> (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to stop receiving such messages;
>
> (b) require the consent, as specified according to its laws and regulations, of recipients to receive commercial electronic messages; or
>
> (c) otherwise provide for the minimization of unsolicited commercial electronic messages.

2. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages who do not comply with its measures implemented pursuant to paragraph 1.9

3. The Parties shall endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

Hong Kong also joined UCENet. However, Hong Kong has difficulty in enforcement of the

domestic laws against overseas senders.

3.1.8. India

A. Definition of spam

India does not have any comprehensive laws regulating spam, and there is no formal definition of spam.

B. Current status for spam response

In case of India, current status for spam response is not identified.

C. Legislation related to spam

India does not have comprehensive laws regulating spam. However, one provision of the Information Technology Act (IT Act 2000, amended in 2008) has the effect of regulating the content of e-mails. Article 66A (c) of the Act stipulates that any person who sends any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable.

Article 66A. Punishment for sending offensive messages through communication service, etc.– Any person who sends, by means of a computer resource or a communication device,–

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance,

inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or

inconvenience or to deceive or to mislead the addressee or recipient about the origin of such

messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation–For the purposes of this section, terms “electronic mail” and “electronic mail message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message

D. Spam policy

In case of India, spam policy is not identified.

E. International cooperation

In case of India, current status for international cooperation regarding spam is not identified.

3.1.9. Indonesia

A. Definition of spam

Indonesia did not have laws regulating spam, and there had been no formal definition of spam. However, in 2021 Indonesia enacted Ministerial Decree Number 5 to regulate marketing SMS and this Decree covers SMS that is for offerings/marketings, sent by cellular mobile network operator, including business entities that cooperate with the organizers cellular mobile network; and/or content provision service providers.

B. Current status for spam response

Indonesia has the current issue regarding law enforcement with spam due to so many spams occur every day.

Therefore, when APT provides programs to enhance the capacity of member countries, Indonesia responded that programs such as training to government officials and consulting through APT Expert Mission are needed. In the case of training, 1) global norms and trends, 2) best practices, recent development, etc., and 3) interactive workshops on solutions are particularly necessary. And, Indonesia answered that the main target of the training should be the manager level government officers in charge of spam-related issues and researchers in public research agency.

In case of consulting, Indonesia answered that information sharing from the experts dispatched by APT is the most needed help.

The government of Indonesia and telecommunication service providers are mainly engaged in anti-spam activities. The government doesn't have any information on the anti-spam activities that private sectors are doing currently.

C. Legislation related to spam

1)Content of spam regulation

Indonesia does not have any comprehensive acts regulating spam. However, one provision of the Law on Information and Electronic Transactions (Indonesia Internet Law, 2008) has the effect of regulating the content of e-mails offering to sell goods and services. Article 9 of the Act stipulates that when goods and services are offered for sale through electronic system, the person offering the sale must provide complete and correct information about the terms of the contract, the manufacturer, and the product which is offered.

Article 9

Business actors who offer products through the Electronic System must provide:

complete and correct information regarding the terms of the contract, the manufacturer, and the product which is offered.

Also, as mentioned above, in 2021 Indonesia enacted Ministerial Decree Number 5 to regulate marketing SMS and this Decree covers SMS that is for offerings/marketings, sent by cellular mobile network operator, including business entities that cooperate with the organizers cellular mobile network; and/or content provision service providers.

According to the Decree, Cellular mobile network operator and/or Content provision service providers are required to provide choice to Telecommunications Service subscribers on the network cellular mobile to refuse delivery of messaging services short message service (SMS).

In the case of Telecommunications Service Subscribers on the network cellular mobile chooses to deny delivery of the service short message service (SMS), mobile network operator cellular and/or content provision service providers Prohibited from sending short message services services/SMS).

So, Indonesia basically stipulates an opt-out system for spam messages, SMS.

2) Regulatory authority

The Ministry of Communications and Information, Indonesia, handles spam related legal issues.

D. Spam policy

1) Technical response

In case of Indonesia, currently they don't have any technical response for spam prevention due to the lack of resources (information, experts, fund, etc.)

2) Self-regulation

In case of Indonesia, currently they don't have any self-regulation scheme for spam prevention and don't have any plan for it.

3) Education/ Awareness raising

In case of Indonesia, education and awareness raising policy for spam prevention is now under implementation. However, they don't have any private sector initiatives related to the education and awareness raising on spam.

E. International Cooperation

Indonesia didn't join the UCENet, but they signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.1.10. Japan

A. Definition of spam

In Japan, "Specified Electronic Mail" means spam in general.

"Specified Electronic Mail" means Electronic Mail sent by a person who sends Electronic Mail (limited to transmissions from telecommunications facilities in Japan or transmission to

telecommunications facilities in Japan; the same shall apply hereinafter) (limited to an organization for profit and a person in cases where the person is engaged in business; hereinafter, "sender") as a means of advertisement or propaganda for their own sales activities or for others.

B. Current status for spam response

In case of Japan, current status for spam response is not identified.

C. Legislation related to spam

1) Key concepts

(1) ″Electronic Mail” means telecommunications to transmit information, including texts, to specified persons by having the screens of communications terminals (including input/output devices; the same shall apply hereinafter) used by said specified persons display said information, and which uses communications methods specified in the applicable Ministry of Internal Affairs and Communications (hereinafter, "MIC") ordinance.

(2) ″Specified Electronic Mail” means Electronic Mail, which a person who sends Electronic Mail (limited to transmissions from telecommunications facilities in Japan or transmission to telecommunications facilities in Japan; the same shall apply hereinafter) (limited to an organization for profit and a person in cases where the person is engaged in business; hereinafter, "sender") sends as a means of advertisement or propaganda for their own sales activities or for others.

So, in Japan, “Specified Electronic Mail” means spam emails and spam messages (SMS/MMS) in general.

2) Contents of spam legislation

(1) Regulatory framework

The Japanese government basically stipulates an opt-in system for spam e-mails and spam messages (SMS/MMS). There are no restrictions on spam calls.

Japan passed the Anti-Spam Act in 2002 and it has been amended several times.

The Act on the Regulation of Transmission of Specified Electronic Mail (hereafter, the Specified Electronic Mail Act) launched an opt-out system in relation to unsolicited email advertisements sent for business purposes, but it was converted to an opt-in system with the revision in 2008.

The Act applies to all commercial mails sent from Japan or to Japan by interest groups or individuals involved in business. Therefore, the law currently applies to senders who send electronic mail to recipients in Japan, wherever the sender is located.

(Limitation of sending electronic mail) Under the Specified Electronic Mail Act, senders may only send commercial e-mails if the recipient falls under the following categories:

(i) Individuals who have informed the sender in advance of their consent to request or receive commercial emails;

A person who has notified the sender or the consignor of transmission (referring to a person who consigned transmission of Electronic Mail) of the request or the consent to send Specified Electronic Mail prior to the transmission.

(ii) The individual who provided his or her email address to the sender;

In addition to those listed in the preceding item, a person who has notified, as specified in the applicable MIC ordinance, the sender or the consignor of transmission of his/her own Electronic Mail Address.

(iii) Individuals who have a prior business relationship with the sender;

In addition to those listed in the preceding two items, a person who has a business relationship with a person engaged in sales activities relating to advertisement or propaganda that employs the said Specified Electronic Mail as its means.

(iv) Individuals or groups who have publicly disclosed their e-mail addresses (only related to profit activities);

In addition to those listed in the preceding three items, an organization or a person who has made, as specified in the applicable MIC ordinance, his/her address public (limited to those who engage in business in the case of a person)

Since all of these categories require active action by the recipient before the sender is allowed to send commercial electronic mail, Japan has essentially adopted an opt-in system for regulating commercial electronic mail.

(Record keeping) A person who has received the notification shall maintain, as specified in the applicable MIC ordinance, a record that proves the fact that a request was made to send Specified Electronic Mail or that consent was made to send Specified Electronic Mail.

(Respect of opt-out) When a sender has received notice of a request not to send Specified Electronic Mail (or, in cases where the request was not to send Specified Electronic Mail pertaining to certain matters, the said request) from any person in accordance with the applicable MIC ordinance, the sender shall not send Specified Electronic Mail against the notifying party's intention indicated in the said notice.

Senders may not send commercial electronic mails to recipients to whom they have been requested to opt-out. There is no grace period for compliance with this request.

(2) Labelling

Commercial electronic mails must contain the sender's name and title, as well as an e-mail address that recipients can use to make opt-out request. These items must be clearly marked so that they can be seen on the recipient's screen.

(Obligation of Labeling) 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

(3) Other regulation

(Prohibition of Transmission under False Sender Information)

Any sender shall not send Electronic Mails, as a means of advertisement for their own or other's sales activities, falsifying the following information of the sender (hereinafter referred to as "sender information") among information for sending and/or receiving Electronic Mails:

(i) Electronic Mail Address used for sending said Electronic Mails
(ii) Codes, including characters, numerical characters, and marks, for identifying telecommunications facilities for sending said Electronic Mails

(Refusal to Provide Telecommunications Services) A telecommunications carrier may refuse to provide Electronic Mail Services to a person who sends Electronic Mails that have a risk of causing following disturbances, to the extent necessary to prevent disturbances, in cases where an Electronic Mail using false sender information has been sent, when it is deemed that there is a risk of causing disturbances in offering smooth Electronic Mail Services, or causing disturbances upon transmission and reception of Electronic Mails to users of the services, where many Electronic Mails being sent to Fictitious Electronic Mail Addresses, or where it is deemed that there are justifiable grounds to refuse the provision of Electronic Mail Services to prevent the occurrence of disturbances.

(4) Regulation on address harvesting software

Specified Electronic Mail Act also prohibits the use of programs that generate random virtual email addresses. Senders must not send mail to e-mail addresses created by using programs that automatically combine symbols, letters, and numbers to generate e-mail addresses.

(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.

3) Regulatory authority

The management responsibility for unsolicited commercial messages rests with the Ministry of Internal Affairs and Communications (MIC). MIC is responsible for the enforcement of laws governing the transmission of specified electronic mails, including e-mail and SMS/MMS. And MIC advocates a zero-tolerance approach to violations of the Act, which prohibits sending unsolicited electronic commercial messages.

MIC is supported by industry initiatives such as the Anti-Spam Consultation Center (ASCC) established by MIC to collaborate with the private sector information and communications industry (e.g., Japan Data Communications Association, JADAC). The ASCC is an independent organization that works as a middle-man and distributes spam reports it receives appropriately (including to MICs for enforcement). MIC has approved JADAC as the

designated body responsible for determining the adequacy of specified electronic mails sending.

Japan does not regulate telephony or facsimile communication, except that telephone or fax falls under the field of telemarketing consumer law and is covered by the Act on Specified Commercial Transactions with respect to the content of the messages.

4) Penalties

If a sender violates the Specified Electronic Mail Act, the Minister of Internal Affairs and Communications may order the sender to take action to comply with the Act. The sender can be fined up to one million yen or imprisoned for up to one year if the sender violates this administrative order.

(Administrative Order)

Where the Minister of Internal Affairs and Communications (hereinafter referred to as "Minister") deems that with respect to transmission of Electronic Mails, including simultaneous transmission of Specified Electronic Mails to many persons, a sender does not comply with the Act, or where the Minister deems that a sender has sent Electronic Mails to Fictitious Electronic Mail Addresses or Electronic Mails using false sender information, and when the Minister deems that it is necessary for preventing the occurrence of disturbances upon transmission and reception of Electronic Mails, the Minister may order said sender to take necessary measures for improvement of the methods for Electronic Mail transmission.

The Minister of Internal Affairs and Communications may require the sender to submit a report on the transmission of commercial mail, and may inspect the sender's business, books, and other records. If the sender refuses to submit such a report or cooperate with an investigation, he/she may be punished by up to 300,000 yen.

In addition, the sender may be subject to additional penalties if his/her agent violates the provisions of the Act. If the sender's agent violates an administrative order of the Ministry of Internal Affairs and Communications to comply with the Act, he or she may be subject to a fine of up to 30 million yen.

D. Spam Policy

In case of Japan, Spam policy is not identified.

E. International Cooperation

Japan has joined UCENet. Also, Japan signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.1.11. Kiribati

A. Definition of spam

Kiribati does not have any law governing SPAM, however the Cybercrime Act 2021 cover in principle the nature of SPAM relating to unauthorized computer system access or unauthorized computer system interference should the SPAM carry a malicious payload to a computer system, interfering with its normal operation.

There is no explicit definition on their national law but presume the cybercrime act 2021 covers the nature of SPAM.

Kiribati has the current challenges regarding the legislation and technical issues with spam and Ministry of Information, Communication, Transport and Tourism Development (MICTTD), Kiribati is in charge of this issue.

B. Current status for spam response

The government of Kiribati is mainly engaged in anti-spam activities. They don't have any information on the anti-spam activities that private sectors are doing currently. The government of Kiribati identifies spam by types of contents, for example, loan/financial assistance, and their anti-spam activities mainly target elderly people.

C. Legislation related to spam

There is no general anti-spam act, but the government of Kiribati believe they need the general anti-spam law and has plan to legislate one. They are still in the stage of planning but expect to have a general anti-spam law in 3-5 years.

D. Spam policy

1) Technical response

The government of Kiribati doesn't have any technical measures to prevent spam. However, Kiribati has a plan to implement technical solutions from government side. They are still in the stage of planning.

2) Self-regulation

There is no anti-spam self-regulation scheme in Kiribati. However, Kiribati has a plan to create

self-regulation scheme. They are worrying about the lack of resources (information, experts, funds, etc.).

3) Education/ Awareness raising

There is no anti-spam policy related to the education and awareness-raising on spam in Kiribati. But the government of Kiribati has a plan to create education and awareness-raising policy that mainly targets local community, and they are in the stage of planning. Preparing for this, they are worrying about the lack of resources (information, experts, funds, etc.).

E. International cooperation

Kiribati doesn't participate in any international cooperation initiatives on spam. However, Kiribati has a plan to create an international cooperation initiative and it is at the stage of planning. They are worrying about the lack of resources (information, experts, funds, etc.).

3.1.12. Republic of Korea

A. Definition of spam

"Spam" refers to "commercial information for profit that is transmitted unilaterally through the information and communication network without the explicit prior consent of the recipient". This definition of spam is stated in the preventing illegal spam guide of the Act on Promotion of Information and Communication Network Utilization and Information Protection.

B. Current status for spam response

1) Current status of categorization

KISA receives spam reports from recipients(users) and is separating the types as follows: Email spam, mobile phone voice spam, mobile phone text spam, SNS spam, bulletin board spam, etc.

KISA is separating the routes of spam traffic as follows:

1. Mobile phone voice spam from;

    - Wired phone service

- Internet phone service
- Mobile phone service
- International call service

2. Mobile phone text spam from;
   - Mass text message service
   - Mobile phone service
   - etc. (Wired phone service, Internet phone service, etc.)

3. Email spam from;
   - Email spam from Korea (Domestic ISP)
   - Email spam from abroad

2) Number of reporting

In 2019, 36,883,787 spam reports were received. In 2020, 42,502,471 spam reports and in 2021(Jan-Aug), 30,249,410 reports were received.

In the second half of 2020, the amount of spam sent increased by 18% compared to the previous year, and in particular, mobile phones voice spam on loan exploded. Also, email spam from overseas has increased.

		Amount fluctuation	**2020 first half**	**2020 second half**
Mobile phone voice spam	sent	35.1% (2,890,000) increase	8,210,000	11,100,000
	Received (one person per day)	0.02 increase	0.07	0.09
Mobile phone text (SMS/MMS) spam	Sent	6.5% (420,000) decrease	6,490,000	6,070,000
	Received (one person per day)	0.10 increase	0.09	0.19
Email spam	Sent (from Korea)	287.2% (280,000) increase	100,000	380,000
	Sent (from abroad)	18.3% (3,750,000) increase	20,560,000	24,310,000
	Received (one person per day)	0.13 decrease	0.31	0.18

The increase in illegal loans and gambling spam exploiting the economic recession caused by the prolonged COVID-19 crisis. So, KISA classify illegal spam as follows: Illegal loan, adult contents, Finance, Communication subscription, Gambling, etc.

C. Legislation related to spam

1) Key concepts

Spam is defined as "advertisement information for the purpose of profit" in the Act on Promotion of Information and Communication Network Utilization and Information Protection (hereinafter, Information and Communications Network Act).

Spam refers to "advertisement information for profit that is transmitted unilaterally through the information and communication network without the explicit prior consent of the recipient". This definition of spam is stated in the preventing illegal spam guide of the Information and Communication Network Act.

Target of the Act

Article 50 Paragraph 1 of the Act stipulates that 'anyone' shall not transmit advertisement information for commercial purposes without the express prior consent of the recipient. Therefore, "a person who transmits" advertising information, regardless of whether it is a corporation, organization, or individual, can be the main subject of this provision. In this case, there is no problem if the person who sent the advertisement information and the advertiser (seller) are the same, however if the sender and the advertiser are different, the question is that who is the subject of this clause. The sender may transmit advertising information in the position of a trustee on behalf of the advertiser.

According to the Information and Communications Network Act, a person who has entrusted the transmission of advertising information to another person shall manage and supervise the person entrusted with the work so as not to violate Article 50. In respect of liability for damages incurred by the person entrusted with the transmission of advertising information (the trustee) in violation of the law in relation to the business, the trustee shall be regarded as an employee belonging to the person who entrusted the transmission of advertising information. In addition, not only those who violate Article 50, but also those who allow them to do so are also subject to a fine not more than 30 million won (approximately USD 30,000).

2) Contents of spam legislation

(1) Regulatory framework

The Korean government basically stipulates an opt-in system for spam emails, spam messages, and spam calls.

Korea's Anti-Spam Act is the Information and Communications Network Act. The Information and Communications Network Act sets the minimum procedural requirements for legal online transmission. In Korea, the transmission of advertisements against the recipient's will is strictly prohibited. The Korean government has made continuous efforts to reduce spam since 1999 and has been monitoring the effectiveness of the implementation of additional provisions. In Korea, the transmission of advertising information using electronic transmission media was first regulated from the 1999 Information and Communications Network Act. Unlike the United States and Europe at that time, where opt-in was applied to automatic outgoing telephone calls and faxes and opt-out was applied to e-mail, Korea did not distinguish between transmission media and applied opt-out for all forms of advertising information using electronic transmission media. The opt-in was applied to telephone and fax from 2005, and from 2014 the opt-in was applied to all advertising information, including e-mail.

If anyone wants to transmit advertisement information for profit using an electronic transmission medium, he/she must obtain the prior consent of the recipient. In this case, the electronic transmission medium refers to a medium that transmits codes, texts, voices, images, or videos to the recipient in electronic form through the information and communications network. Since “transmission medium” is a technology-neutral and open concept, it is not limited to phone calls, faxes, and e-mails if it is transmitted electronically, and messaging functions such as apps, SNS, blogs, and cafes can also fall under the electronic transmission medium.

The Information and Communications Network Act regulates “advertising information for profit”. Terminologically, the scope of regulation can be considered very narrow compared to other countries, but in practice, it is considered that 'in principle, all information sent by salespeople to customers is advertising information', so actually the subject of discipline is very wide.

If a person who has directly collected contact information from the recipient through a transaction relationship intends to transmit commercial advertising information about the same type of goods/services that he or she handles and trades with the recipient within 6 months from the end of the transaction relationship, the recipient’s consent will not be needed. Since “transaction relationship” means a relationship of buying and selling goods/services, barter exchange is included in the transaction, but gift or free service is not a transaction. Therefore, the sender’s obligation to get consent is not exempted even though the sender collected the recipient's contact information by providing gift or free services.

The sender’s obligation to get consent is not exempted when the contact information collected directly from the recipient without transaction relationship, as it must be the contact

information collected through “transaction relationship”. In other words, when a specific transaction has not been made after registering for a website membership, when the recipient puts items of interest in the shopping cart of an internet shopping mall and does not make payment, when the recipient has a record of using the online search service for a specific product but a specific transaction has not been made, in these cases the sender’s obligation to get consent is not exempted because the actual transaction for the product has not been made.

(Prohibit transmission when the recipients refuse to receive) 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.

(Regular checking of consent to receive) A person who obtains consent to receive advertising information shall regularly verify whether an addressee of advertising information consents to receive such information, as prescribed by Presidential Decree.

(Sender information and unsubscribe facility) A person who transmits advertising information for profit by using an electronic transmission medium shall specify the following matters in advertising information, as prescribed by Presidential Decree:

1. The name and contact details of a sender;

2. Matters regarding measures and methods by which an addressee can readily express his or her intention to refuse to receive information or to revoke his or her consent to receive information.

(2) Labelling

“(Advertising)” must be indicated at the beginning of the title or advertisement information.

(3) Regulation on address harvesting software

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;

3) Regulatory authority

The Korea Communications Commission (KCC) and the Korea Internet & Security Agency (KISA) are in charge of spam, while the Financial Supervisory Service and the Korean National Police Agency are in charge of voice phishing. KISA delivers spam report data to the agency (National Gambling Control Committee, Korea Exchange, etc.) in charge of each spam type and uses it to block spam.

4) Penalties

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.

The Act on Promotion of Information and Communications Network Utilization and Information Protection stipulated the punishment and penalty regulations for spam sending as follows:

Article 74

(1) Any of the following persons shall be punished by imprisonment with labor for up to one year or by a fine not exceeding 10 million won:

A person who transmits any advertising information, in violation of this law

Article 76

Any of the following persons and a person who made a third party commit an act falling under subparagraphs, shall be punished by an administrative fine not exceeding 30 million won:

A person who transmits any advertising information for profit, without the explicit consent of the recipient.

A person who fails to state the matters required to be stated, or who states false information on such matters, when he/she transmitted any advertising information.

A person who makes an addressee bear the burden of any expense.

A person who fails to verify whether an addressee gives consent to receive advertising information.

A person who installs an advertising program for profit without consent of the relevant user.

A person who posts any advertising information for profit on an Internet webpage.

D. Spam policy

1) Technical response

The Act on Promotion of Information and Communications Network Utilization and Information Protection stipulated the Distribution of Software Designed to Block Transmission of Advertising Information for Profit as follows:

(Distribution of Software Designed to Block Transmission of Advertising Information for Profit) The Korea Communications Commission may develop and distribute software or computer programs designed for addressees to conveniently block or report any advertising information for profit.

The Korea Communications Commission may provide necessary support to related public agencies, corporations, organizations, or similar for facilitating the development and distribution of software or computer programs for blocking or reporting transmission.

If telecommunications services rendered by a provider of information and communications services are used in transmitting advertising information for profit, the Korea Communications Commission may recommend the provider of information and communications services to take necessary measures, such as development of technology, education, and public relations activities to protect addressees.

KISA provides various technical support to telecommunication service providers. KISA-RBL (Realtime Blocking List), KISA-MRBL (Mobile Realtime Blocking List), White Domain(kind of white list; A system that guarantees e-mail transmission to major domestic portal sites only for pre-registered individuals or businesses), SPF (Sender Policy Framework; kind of authentication technology which ensures the recipient can check whether the information of the actual mail server matches the sender information displayed in the e-mail by publicly registering mail server information in DNS in advance) are applied to reduce spam technically.

Also, telecommunication service providers operate the Intelligent spam blocking system.

2) Self-regulation

In Korea, the cooperative system between the government, telecommunication service providers, and industry associations in relation to spam response is relatively well established. A representative example is the Spam Distribution Status Report, which has been issued every half year since 2012. By regularly announcing the amount of spam distribution of mobile service providers or e-mail service providers, the voluntary efforts of telecommunication service providers to reduce spam are enhanced.

To this end, indexes that can compare the degree of effort to reduce spam distribution for each telecommunication service provider involved in the spam transmission process are derived and operated.

- (Cell phone) The amount of spam received by each mobile service provider, the amount of sending spam by each wired/wireless phone service provider, Biz-SMS service provider, Internet phone service provider, etc.
- (E-mail) The amount of spam received per e-mail account by major portal service, the amount of spam sent by network operator such as ISP, etc.

In addition, the government suppresses the sending of spam by strengthening the sense of responsibility of telecommunication service providers.

3) Education/ Awareness raising

For business operators, government provides business briefing sessions and educational content to prevent illegal spam transmission.

For recipients(users), government produces and distributes educational materials and educational contents to block and prevent illegal spam.

E. International cooperation

The Korean government participated in the GSMA Spam reporting service (2011) and informed the international community of the excellence of Korea's anti-spam technology and system and expanded international cooperation.

The GSMA spam reporting service is a project to build a global reporting system that collects mobile spam information from around the world and analyzes major statistics and trends. The domestic mobile phone spam report information received through the report system is delivered to the GSMA, and overall statistics and trend analysis results are provided.

In addition, the Korean government joined the London Action Plan and UCENet and served as a member of the Executive Committee (composed of Korea KISA, US FTC, UK ICO, Netherlands ACM, New Zealand DIA, Canada CRTC). There is a Memorandum of Understanding Among Public Authorities of the Unsolicited Communications Enforcement Network Pertaining to Unlawful Telecommunications and Spam.

The Korean government established the “UCENet Asia-Pacific” in 2018 and has been serving as its chairperson, and five countries (Korea, Australia, Japan, New Zealand, and Taiwan) attended the inauguration ceremony. It has a close mutual cooperation plan, such as sharing illegal spam data collected from each country with member countries and restricting service use of illegal overseas spam senders. Also, Korea signed the Regional Comprehensive

Economic Partnership (RCEP) agreement.

Korea thinks that cross-border cooperation to block international voice/text spam and global messenger spam (e.g., iMessage) is the most important challenges.

3.1.13. Lao PDR

A. Definition of spam

Lao PDR does not have any comprehensive law governing SPAM, however in Laos spam message is included in the definition of "fraud message" which mentioned on the Ministerial Decree of Interconnection and Services of Messages. This is available on Lao version only (No.2597/MTC; on 12 August 2022).

However, it has the Memorandum of understanding which mentioned about the spamming calls (voice spam), that is an agreement to handle the voice spamming calls between Lao National Internet Center and Telecommunication services.

B. Current status for spam response

The spamming calls statistic has more than 400,000 calls per year such as between 2019 and 2020. This was the peaking time of the spamming call period, However, these days the number of spamming calls decreased slightly.

Regarding the source of spam, it could be found source route come from neighboring countries that relate to Lao National Internet Center gateway, and found that the source prefix of mobile phone number come from African continent, especially the countries have high-rate charge for voice calls. SMS spam come from overseas applications like the content will have hypertext link that persuaded customer to click it.

Laos has the current challenges regarding international cooperation with spam. Lao National Internet Center is in charge of spam issue, and it assumed that there are some grey routes traffic that international partners would not be able dealing with this issue effectively.

Therefore, when APT provides programs to enhance the capacity of member countries, Laos responded that programs such as training to government officials, policy consulting through the APT Expert Mission are needed. In the case of training, 1) global norms and trends, 2) specific rules and regulations,3) best practices, recent development, etc., and 4) interactive workshops on solutions are particularly necessary. And Laos answered that the main target of the training should be the manager level government officers in charge of spam-related issues or researchers in public research agency.

In the case of policy consulting, they answered that they need drafting new anti-spam act, drafting amendment to current law, and drafting strategic plan for anti-spam from experts dispatched by APT the most.

The government of Laos and telecommunication service providers are mainly engaged in anti-spam activities. The government doesn't have any information on the anti-spam activities that private sectors are doing currently.

C. Legislation related to spam

There is no general anti-spam act, but the government of Laos believes they need the general anti-spam law and has plan to legislate one. They are still in the stage of research but expect to have a general anti-spam law in 3-5 years.

D. Spam policy

1) Technical response

The SMS spam is filtered by the SMS inspection system. Spamming calls will be defined by the monitoring systems that developed by Lao engineers.

2) Self-regulation

There is no anti-spam self-regulation scheme in Laos. However, the government of Laos has a plan to create self-regulation scheme. They are worrying about the lack of resources (information, experts, funds, etc.).

3) Education/ Awareness raising

There is no anti-spam policy related to the education and awareness-raising on spam in Laos. But, the government of Laos has a plan to create education and awareness-raising policies and they are in the stage of research. Preparing for this, they are worrying about the lack of resources (information, experts, funds, etc.).

E. International cooperation

Laos signed RCEP Agreement, and Laos has a plan to create an international cooperation initiative and it is at the stage of research. They are worrying about the lack of resources

(information, experts, funds, etc.).

3.1.14. Malaysia

A. Definition of spam

There are no direct regulations on spam in Malaysia. However, Article 233 of 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" as spam.

B. Current status for spam response

In case of Malaysia, current status for spam response is not identified.

C. Legislation related to spam

1) Key concepts

In Malaysian laws, there are no direct concepts related to spam.

2) Contents of spam legislation

(1) Regulatory framework

Malaysian law basically does not have specific regulations related to spam e-mails and messages, so there is no opt-in or opt-out system.

However, as we saw earlier, Article 233 of the Communications and Multimedia Act prohibits "communications sent to a specific number or electronic address, whether persistent, repetitive, or otherwise, with the intention of annoying or harassing another person, or comments, requests, suggestions or other communications sent with an inappropriate and offensive nature and with the intention of annoying or harassing another person". So, above said communications violate the Act.

233. Improper use of network facilities or network service, etc.

(1) A person who

(a) by means of any network facilities or network service or applications service knowingly makes, creates, or solicits; and initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or

(b) initiates a communication using any applications service, whether continuously, repeatedly, or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address, commits an offence.

The intent underlying Section 233 may be utilized to deal with spam. It may be an appropriate section to deal with the problems faced by spamming activities.

Notwithstanding, to fall within the scope of the section however the communication must have been initiated with the intention of annoying, abusing, threatening, or harassing a person. In cases of spamming, the consequences or effect of such communication may be that the recipients are annoyed, harassed or abused. However, it may be difficult to argue that this was the intention of the sender. The requirement or kind of "intent" the section requires may not always exist or be difficult to determine.

This may give rise to enforcement problems, bearing in mind that the onus of proof is on the prosecution. Further, such intention may not exist given that people who initiate such communication for marketing and advertising purposes are unlikely to initiate such communication with the intent to annoy abuse, threaten or harass potential clients.

Section 233, however, may be seen as being inadequate in some aspects, for instance:

1. There are no provisions in this section that allow a person to opt in or opt out to

receive unsolicited Internet e-mail or short messages;

2. There is no requirement that all electronic messaging contains accurate details

of the sender's name and address;

3. There are no civil sanctions for unlawful conduct including financial penalties and

ability to seek enforceable undertakings and injunctions to minimize

the proliferation of spamming.

In addition, in June 2005, Malaysia Communications and Multimedia Commission (MCMC) registered a sub-code describing how Internet access service providers should deal with spam.

Developed by the Communications Multimedia Customer Forum, this sub-code obligates service providers to develop documented procedures for handling spam incidents and make information on anti-spam measures available on their websites. The sub-code also suggests that service providers should consider (but not be obligated to) include in their contracts with customers prone to generating spam: (1) prohibiting sending spam messages; (2) an agreement that sending spam may result in suspension or termination of the customer's account; (3) A usage policy to ensure that customers include accurate header information, valid return email addresses, working unsubscribe facility, sender information and appropriate labeling for all commercial emails sent by them.

(2) Labeling

Although not directly stipulated in the Act, MCMC's sub-code to Internet access service providers is proposing that service providers should consider including in their contracts with customers a usage policy that ensures that customers include appropriate labeling for all commercial emails sent by them.

3) Regulatory authority

Malaysia Communications and Multimedia Commission (MCMC) is in charge of spam regulation in Malaysia.

4) Penalties

Violators of the Act face a fine of up to RM50,000 and imprisonment not exceeding one year. Repeat offenders may face an additional fine of RM1,000 per day for offenses made after conviction.

Section 233.

(3) A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day during which the offence is continued after conviction.

D. Spam policy

1) Technical response

In case of Malaysia, technical response for spam prevention is not identified.

2) Self-regulation

In case of Malaysia, self-regulation for spam response is not identified.

3) Education/ Awareness raising

MCMC's approach in this regard is self-management by users and management of service providers through education and awareness-raising activities. A four-tier strategy to address spam is implemented.

- Tier 1: Self-management by users
- Tier 2: Complaints against service providers
- Tier 3: If the complaint is not resolved, file a complaint to the Malaysian Consumer Forum
- Tier 4: If not resolved yet, transfer to MCMC

E. International cooperation

The Malaysian government joined UCENet, an international spam response cooperation initiative. Also, Malaysia signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.1.15. Micronesia (Federated States of)

A. Definition of spam

The definition of "Unsolicited Commercial Messages" is not contained in Federated States of Micronesia (FSM) National law or regulation because FSM law or regulation does not address or define spam.

B. Current status for spam response

FSM has no reporting system or mechanism for measuring spam traffic in FSM. There is no unified approach to the issue of SPAM in FSM.

In FSM telecommunication service providers are mainly engaged in anti-spam activities.

C. Legislation related to spam

There is no general anti-spam act and no plan to legislate general anti-spam act because of lack of resources (information, experts, funds, etc.).

D. Spam policy

1) Technical response

FSM Telecom Corporation is conducting technical measures to prevent spam. From the government side, FSM implemented no anti-spam technical solutions. And, FSM doesn't have a plan to implement technical solutions from government side because of lack of resources (information, experts, funds, etc.).

2) Self-regulation

There is no anti-spam self-regulation scheme in FSM. And, FSM doesn't have a plan to create self-regulation scheme because of lack of resources (information, experts, funds, etc.).

3) Education/ Awareness raising

There is no anti-spam policy related to the education and awareness-raising on spam in FSM. And, FSM doesn't have any plan to create education and awareness-raising policy because of lack of resources (information, experts, funds, etc.).

E. International cooperation

FSM doesn't participate in any international cooperation initiatives on spam. FSM doesn't have any plan to participate any international cooperation initiatives because of lack of resources (information, experts, funds, etc.).

3.1.16. Nepal

A. Definition of spam

In case of Nepal, they don't have any comprehensive law on spam. However, they define spam as 'irrelevant or unsolicited messages' in cybersecurity guidelines.

B. Current status for spam response

In Nepal, government issues awareness notice to tackle spam, and they recognized email, SMS, web portal and screen saver as the source/routes of spam traffic. however, they don't have statistical measurement regarding volume of spam traffic or spam report.

Government, Telecommunication Service Providers, Industry associations and non-governmental organizations are engaged in anti-spam activities in Nepal, but detailed information on private sector anti-spam activities is not identified.

In the case of Nepal, survey result shows that there are issues related to the legislation, law enforcement, international cooperation, lack of awareness and in adequate cybersecurity education regarding spam.

Therefore, when APT provides programs to enhance the capacity of member countries, Nepal responded that programs such as training to government officials and consulting through APT Expert Mission are needed. In the case of training, 1) an overall overview of the anti-spam legal system, 2) global norms and trends, 3) specific rules and regulations, 4) analysis of current regulations and problems of each APT member country, 5) best practices, recent development, etc., 6) Interactive workshop for finding solutions are particularly necessary. Regarding the consulting, Nepal answered that drafting new Anti-spam Act and drafting strategic plan for anti-spam are needed.

C. Legislation related to spam

1) Key concepts

There is no comprehensive anti-spam legislation in Nepal. However, some kind of spam (e.g., such as spam with fraud or any other illegal act) can be treated as cybercrimes under Electronic Transaction Act 2008.

2) Contents of spam legislation

There is no comprehensive anti-spam legislation in Nepal but currently they have a plan to legislate new act and it is on its planning stage. Nepal administration thinks new act on spam

is very needed and expects the legislation within ten years.

3) Regulatory authority

Nepal Telecommunications Authority (NTA) is in charge of spam, and they cooperate with organizations related to the type of advertisement as and when required or needed. However, the details are not identified.

4) Penalties

There is no comprehensive anti-spam legislation in Nepal. So, they don't have any regulation on spam penalties.

4. Spam policy

1) Technical response

In case of Nepal, they don't implement technical solutions from government side. Also, they don't have any plan to implement a kind of technical solution. They responded that it is because they have never experienced serious spam related issues and don't feel any need. However, Nepal administration thinks telecommunications service providers have the responsibility for countering spam.

2) Self-regulation

Nepal doesn't have anti-spam self-regulation scheme, but the survey shows that they have a plan to create a self-regulation scheme and it is on its planning stage. However, Nepal administration thinks telecommunications service providers have the responsibility for countering spam.

3) Education/ Awareness raising

At present, Nepal doesn't have any education/ awareness raising programs. Also, they don't have any plan to create an education and awareness raising policy. They responded that it is because they have never experienced serious spam related issues and don't feel any need.

E. International cooperation

According to the survey, Nepal hasn't joined any international cooperation initiatives and doesn't have any plan to create new one or join any existing initiatives. The survey shows that it is because they have never experienced serious spam related issues and don't feel any need.

3.1.17. New Zealand

A. Definition of spam

Spam is an unsolicited 'commercial electronic message'. The term 'commercial electronic message' includes electronic messages (e-mails, SMS text messages, instant messages, but excluding voice calls and faxes) that sell goods, services, land, or business opportunities.

B. Current status for spam response

In case of New Zealand, current status for spam response is not identified.

C. Legislation related to spam

1) Key concepts

The term 'commercial electronic message' includes electronic messages (e-mails, SMS text messages, instant messages, but excluding voice calls and faxes) that sell goods, services, land, or business opportunities.

The Act also specifies certain types of messages excluded from the definition of commercial electronic messages, including messages that provide:

- Quotation if requested
- Warranty or product recall information
- Factual information about subscription, member account, or similar relationship;
- Goods or services, including product updates or upgrades, that are intended to be received by the recipient under the terms of the transaction;
- Content for the purpose specified in the regulation under the Act.

More specifically, **commercial electronic message** means an electronic message that

(i) markets or promotes goods; or services; or land; or an interest in land; or a business or investment opportunity; or

(ii) assists or enables a person to obtain dishonestly a financial advantage or gain from another person; or

(iii) provides a link, or directs a recipient, to a message that does 1 or more of the things listed in subparagraphs (i) and (ii); but does not include an electronic message that—

(i) provides a quote or estimate for the supply of goods or services if that quote or estimate was requested by the recipient; or

(ii) facilitates, completes, or confirms a commercial transaction that the recipient previously agreed to enter with the person who authorised the sending of the message; or

(iii) provides warranty information, product recall information, or safety or security information about goods or services used or purchased by the recipient; or

(iv) provides notification of factual information about a subscription, membership, account, loan, or similar relationship involving the ongoing purchase or use by the recipient of goods or services offered by the person who authorised the sending of the message, or the recipient's ongoing subscription, membership, account, loan, or similar relationship; or

(v) provides information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(vi) delivers goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously entered with the person who authorised the sending of the message; or

(vii) provides the recipient with information about goods or services offered or supplied by a government body; or a court or tribunal; or

(viii) has any other purpose set out in the regulations.

(New Zealand link)

A particular message may have a New Zealand link if it originates in New Zealand, if the device used to access the message is within New Zealand, if the recipient is an organization doing business in New Zealand, if the message has been sent to an electronic address where the message ends in '.nz', or if the message was sent to a non-existent electronic address but it reasonably appears that the message was accessed using a device located in New Zealand.

More specifically, an electronic message has **a New Zealand link** if one or more of the following applies:

(a) the message originates in New Zealand:

(b) the person who sent the message is an individual who is physically present in New Zealand when the message is sent; or an organisation whose central management and control is in New Zealand when the message is sent:

(c) the computer, server, or device that is used to access the message is located in New Zealand:

(d) the recipient is an individual who is physically present in New Zealand when the message is accessed; or an organisation that carries on business or activities in New Zealand when the message is accessed:

(e) if the message cannot be delivered because the relevant electronic address does not exist, assuming that the electronic address existed, it is reasonably likely that the message would have been accessed using a computer, server, or device located in New Zealand:

(f) it is sent to an electronic address that ends with ".nz"; or begins with an international access code directly followed by "64".

2) Contents of spam legislation

(1) Regulatory framework

Basically, the New Zealand government has an opt-in system for spam emails and messages. New Zealand's Unsolicited Electronic Messages Act 2007 came into force in September 2007. This law has basically the same structure as Australia's Spam Act. The Act prohibits the sending of unsolicited commercial electronic messages containing New Zealand links.

Key Points for Compliance of Unsolicited Electronic Messages Act 2007

- Commercial electronic messages should not be sent without the prior consent of the recipient.
- All commercial electronic messages must include an "unsubscribe facility" by which the recipient can (at no cost) notify the sender that he or she will not receive such messages in the future.
- All commercial electronic messages must include information about who authorized the sending of the message and how to contact that person.

(Unsolicited commercial electronic messages must not be sent) 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

(Commercial electronic messages must include accurate sender information)

A person must not send, or cause to be sent, a commercial electronic message that has a New Zealand link unless the message clearly and accurately identifies the person who authorised the sending of the message; and the message includes accurate information about how the recipient can readily contact that person.

(Commercial electronic messages must contain functional unsubscribe facility)

A person must not send, or cause to be sent, a commercial electronic message (the principal message) that has a New Zealand link unless the principal message includes a functional unsubscribe facility that the recipient may use to instruct the person who authorised the sending of the principal message (the sender) that no further commercial electronic messages from or authorised by the sender should be sent to the electronic address at which the principal message was received.

(Acquiring consent)

Consent requirements apply to all commercial electronic messages, whether new or existing contacts information. This means that senders of commercial electronic messages must also obtain consent from people who are currently in their existing e-marketing contacts list.

The Act anticipates that a person's consent to receive commercial electronic messages can be explicit, inferred, or otherwise deemed. Explicit consent may be given by the owner of the electronic address or by another person using the relevant electronic address. Inferred consent arises from the conducts, businesses, and other relationships of the people involved. Finally, deemed consent arises from the conspicuous publication of an electronic address in certain circumstances under the regulations made under the Act.

Expressing consent explicitly indicates that the recipient consents to sending the message. Regarding inferred consent, the federal court in Australia has held that since it is reasonably inferable that a buyer of an email order may want to know about the supplier's business (in the absence of evidence to the contrary), the buyer's consent to receive future emails can be reasonably inferred. However, the court also recognizes that whether consent can be inferred from the relationship between the sender and the recipient is a matter of fact and particular circumstance.

The deemed consent clause only applies if:

- When the recipient's electronic address is disclosed

- If the disclosure is not accompanied by a statement such as “no spam”, etc.

Conversely, if you use your email address on a business website, you must include a "no spam" statement to avoid being considered as giving your consent.

Unsolicited Electronic Messages Act

4. Interpretation

(1) consented to receiving means

(i) express consent, whether given by the relevant electronic address-holder or any other person who uses the relevant electronic address; or

(ii) consent that can reasonably be inferred from the conduct and the business and other relationships of the persons concerned; and any other circumstances specified in the regulations; or

(iii) consent that is deemed to have been given when the following circumstances apply:

(A) an electronic address has been conspicuously published by a person in a business or official capacity; and

(B) the publication of the address is not accompanied by a statement to the effect that the relevant electronic address-holder does not want to receive unsolicited electronic messages at that electronic address; and

(C) the message sent to that address is relevant to the business, role, functions, or duties of the person in a business or official capacity;

But does not include the circumstances specified in the regulations from which consent cannot be inferred.

(2) Regulation on address harvesting software

The Act also prohibits the use of harvested electronic address lists or electronic address harvesting software intended to send unsolicited commercial electronic messages in violation of the Act.

Unsolicited Electronic Messages Act Subpart 2

13. Restriction on use of address-harvesting software and harvested-address lists

(1) 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.

3) Regulatory authority

Department of Internal affairs is in charge of spam regulation in New Zealand.

4) Penalties

Persons affected by the violation of the Act may seek an injunction from the High Court or may apply to a district or high court (depending on the amount required) for compensation or damages.

Unsolicited Electronic Messages Act19. Possible responses to civil liability event

If a civil liability event is alleged to have occurred, any person affected by that event may do 1 or more of the following:

(i) seek an injunction from the High Court under section 40 or 42:

(ii) make an application to the court for compensation or damages under section 46:

The law also envisages government-led enforcement by the Department of the Internal Affairs. The Department of the Internal Affairs can sue violators seeking fines of up to NZD 200,000 for individuals and NZD 500,000 for corporations. People who are suffering losses because of spam, including ISPs, can also apply to participate in lawsuits initiated by the Ministry of Internal Affairs in district or higher courts. The Department of Internal Affairs can also issue official warnings, issue civil infringement notices (specifying fines to be paid), seek enforceable undertakings from spammers, or seek injunctions from district or higher courts for enforceable undertakings.

The enforcement department may investigate, and take enforcement action in relation to, an alleged civil liability event if it considers that an investigation or enforcement action is appropriate in the circumstances.

On the application of the enforcement department, the court may order a person (the perpetrator) to pay a pecuniary penalty to the Crown, or any other person specified by the court, if the court is satisfied that the perpetrator has committed a civil liability event.

If the perpetrator is an individual, the court may order the perpetrator to pay a pecuniary penalty not exceeding $200,000 in respect of the civil liability events that are the subject of the enforcement department's application.

If the perpetrator is an organisation, the court may order the perpetrator to pay a pecuniary penalty not exceeding $500,000 in respect of the civil liability events that are the subject of the enforcement department's application.

An enforcement officer may issue 1 or more formal warnings to a person if the enforcement officer has reasonable grounds to believe that that person has committed a civil liability event. Also, if an enforcement officer has reasonable grounds to believe that a person has committed 1 or more civil liability events, the enforcement officer may issue a civil infringement notice relating to those events to that person.

The enforcement department may accept a written undertaking given by a person in connection with commercial electronic messages; or address-harvesting software; or harvested-address lists.

If the enforcement department considers that a person who gave an undertaking has breached 1 or more of its terms, the enforcement department may apply to the court for an order.

If the court is satisfied that the person has breached 1 or more of the terms of the undertaking, the court may make any or all the following orders:

(a) an order directing the person to comply with the relevant terms of the undertaking:

(b) an order directing the person to pay to the enforcement department an amount up to the amount of any financial benefit that the person has obtained directly or indirectly and that is reasonably attributable to the breach:

(c) any order that the court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach:

(d) any other order that the court considers appropriate.

D. Spam policy

1) Technical response

In case of New Zealand, technical response for spam prevention is not identified.

2) Self-regulation

The New Zealand Internet Society (InternetNZ), Telecommunications Forum (TCF), the

Marketing Association and the New Zealand ISP Association (ISPANZ) have published self-regulatory codes of practice for service providers regulated by the Act. In both the Act and the Code, a service provider is defined as a person who provides services, goods, or equipment to enable communications. This Code establishes the minimum acceptable practices for service providers to minimize and manage spam. The Code covers, among other things, working with law enforcement agencies, making spam filters available, reporting requirements and complaint handling processes.

3) Education/ Awareness raising

In case of New Zealand, education and awareness raising activities for spam response is not identified.

E. International Cooperation

New Zealand didn't join the UCENet. However, New Zealand signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.1.18. Pakistan

A. Definition of spam

Spamming means the transmission of harmful, fraudulent, misleading, illegal, or unsolicited messages in bulk to any person without the express permission of recipient or causing any electronic system to show any such message or is being involved in falsified online user account registration or falsified domain name registration for commercial purpose. (Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations 2009).

"unsolicited information" means the information which is sent for commercial and marketing purposes against explicit rejection of the recipient and does not include

marketing authorized under the law (PAKISTAN ELECTRONIC CRIMES ACT, 2016)

B. Current status for spam response

In Pakistan, Pakistan Telecommunication Authority (PTA) identifies and measures spam by subscribers' complaints and PTA also monitor the numbers which receive the SMS spam.

In the case of Pakistan, survey result shows that there are issues related to the technical aspect, law enforcement, international cooperation regarding spam. They answered that fraudulent calls from different countries using fake numbers are received and it is difficult to trace them, so cooperation between countries is important to trace the source of call/SMS.

Therefore, when APT provides programs to enhance the capacity of member countries, Pakistan responded that programs such as training to government officials, policy consulting through the APT Expert Mission are needed. In the case of training, 1) an overall overview of the anti-spam legal system, 2) global norms and trends, 3) specific rules and regulations, 4) analysis of current regulations and problems of each APT member country, 5) best practices, recent development, etc., and 6) interactive workshops on solutions are particularly necessary. And Pakistan answered that the main target of the training should be the director general level or director level government officers in charge of spam-related issues.

In the case of policy consulting, they answered that they need information sharing and drafting strategic plan for anti-spam from experts dispatched by APT the most.

C. Legislation related to spam

1) Key concepts

There is anti-spam law in Pakistan. Spamming is an offence under the Pakistan Electronic Crimes Act 2016. However, it is a little difficult to consider it as a comprehensive anti-spam legislation comparing with other countries' anti-spam legislations.

In the Act, ″unsolicited information" means the information which is sent for commercial and marketing purposes against explicit rejection of the recipient and does not include marketing authorized under the law (PAKISTAN ELECTRONIC CRIMES ACT, 2016)

2) Contents of spam legislation

The Pakistan government basically applies an opt-in system to spam e-mails. The Pakistan Electronic Crimes Act provides the followings.

(Prohibit spamming without permission of the recipient)

A person commits the offence of spamming, who with intent transmits harmful, fraudulent, misleading, illegal, or unsolicited information to any person without permission of the recipient

or who causes any information system to show any such information for wrongful gain.

(Prohibit direct marketing that doesn't have unsubscribe option)

A person including an institution or an organization engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe from such marketing.

3) Regulatory authority

Both Federal Investigation Authority (FIA) and Pakistan Telecommunication Authority (PTA) are cooperating each other in terms of spam response.

4) Penalties

They have penalties for sending spam such as fine, imprisonment, cancellation of short codes, and blocking of numbers/IMEIs, etc. Whoever commits the offence of spamming or engages in direct marketing that doesn't have unsubscribe option, for the first time, shall be punished with fine not exceeding fifty thousand rupees and for every subsequent violation shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to one million rupees or with both.

4. Spam policy

1) Technical response

In the case of Pakistan, it was found that government (PTA) and Telecommunication service providers are mainly engaged in anti-spam activities. Regarding technical response, telecommunication service providers (operators) have installed anti-spam filters. The filters block the marketing SMS to subscriber who has opted not to receive any marketing SMS and numbers or IMEIs who send the marketing SMS.

2) Self-regulation

Pakistan doesn't have anti-spam self-regulation scheme.

3) Education/ Awareness raising

At present, PTA disseminates public awareness messages regarding spamming fraudulent

activities. Also, they put out advertisement in newspaper and TV.

According to the PTA's regulation 32-A, all operators shall transmit messages to all of its consumers/public at large in accordance with minimum requirements set out as under:

For the purposes of these regulations, following shall be termed as "public interest issues"

(f) Fraudulent/Obnoxious/Spamming issues.

E. International cooperation

According to the survey, PTA thinks tracing the source of spamming is the biggest challenge to counter spam effectively cross-border. However, for this purpose, they are not joining in any existing international cooperation initiatives at all. Instead, they have a plan to make an international cooperation initiative.

In addition, the Pakistan Electronic Crimes Act provides the following provisions relating to the international cooperation.

INTERNATIONAL COOPERATION

39. International cooperation.-(1) The Federal Government may upon receipt of a request, extend such cooperation to any foreign government, 24 x 7 network, any foreign agency or any international organization or agency for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under this Act.

(2) The Federal Government may forward to a foreign government, 24 x 7 network, any foreign agency or any international agency or organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offence under this Act.

(3) The Federal Government may require the foreign government, 24 x 7 network, any foreign agency or any international agency to keep the information provided confidential or use it subject to some conditions.

(4) The Federal Government may send and answer requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

(5) The Federal Government may refuse to accede to any request made by a foreign government, 24 x 7 network, any foreign agency or any international organization or agency if the request concerns an offence which may prejudice its national interests including its sovereignty, security, public order or an ongoing investigation or trial or rights of its citizens guaranteed

under the Constitution of the Islamic Republic of Pakistan.

3.1.19. Papua New Guinea

A. Definition of spam

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. (Cybercrime Code Act, 2016)

B. Current status for spam response

In Papua New Guinea (hereinafter PNG), government identifies and measures spam by subscribers' spam reporting. They measure email, SMS/MMS and IP-based application spam and the number of spam reporting is monthly about 10-20. Citizens are not aware of the spam reporting system, so they need to raise the awareness of citizens.

In PNG, government and non-governmental organizations are mainly engaged in anti-spam activities, but the problem is lack of collaboration within the relevant agencies. National ICT Authority (NICTA), ICT regulator of PNG is establishing Memorandum of Understanding with the agencies to address such issues. Also, the telecommunications operators or service providers are required to prevent spam by the Cybercrime Code Act and National Information and Communication Technology Act.

In the case of PNG, survey result shows that there are issues related to the technical aspect, government-private sector cooperation, law enforcement, international cooperation, and public awareness regarding spam. They answered that their challenges are enforcement measures, multi-stakeholder anti-spam efforts, citizen education about the danger of spam and lack of training for law enforcement agency.

Therefore, when APT provides programs to enhance the capacity of member countries, PNG responded that programs such as training to government officials, policy consulting through the APT Expert Mission are needed. In the case of training, 1) an overall overview of the anti-spam legal system, 2) global norms and trends, 3) specific rules and regulations, 4) analysis of current regulations and problems of each APT member country, 5) best practices, recent development, etc., and 6) interactive workshops on solutions are particularly necessary. And, PNG answered that the main target of the training should be the manager level government officers in charge of spam-related issues, school principals and police.

In the case of policy consulting, they answered that they need interview with domestic experts, information sharing from the experts dispatched by APT, drafting new anti-spam act, drafting amendment to current law, and drafting strategic plan for anti-spam.

C. Legislation related to spam

1) Key concepts

There isn't any comprehensive anti-spam legislation in PNG. However, Spamming is an offence under the Cybercrime Code Act 2016.

In the Act, 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. (Cybercrime Code Act, 2016)

2) Contents of spam legislation

The PNG government considers spam (deceiving or misleading users, falsifying header information) as violations of law. However, the Act doesn't regulate opt-in or opt-out scheme. The PNG Cybercrime Code Act provides the followings.

26. SPAM

A person who intentionally and without lawful excuse or justification, or more than a lawful excuse or justification, or recklessly, uses an electronic system or device –

(a) to initiate the transmission of multiple electronic messages with the intent to deceive or mislead users; or
(b) which is password protected to relay or retransmit multiple electronic messages, with the intent to deceive or mislead users, or any ICT Service Provider, as to the origin of such messages; or
(c) to materially falsify header information in multiple electronic messages with the intent of initiating the transmission of such messages,

is guilty of an offence.

The PNG government has a plan to legislate a general act for spam regulation and it is on the planning stage. They expect to legislate one within 3-5 years.

3) Regulatory authority

Department of Police, Department of ICT and National ICT Authority are handling spam related legal issues.

4) Penalties

They have penalties for sending spam such as fine, imprisonment. In the case of a natural person, a fine not exceeding K5,000.00 or imprisonment for a term not exceeding 12 months, or both, and in the case of a body corporate, a fine not exceeding K100,000.00.

4. Spam policy

1) Technical response

In the case of PNG, it was found that government organization, PNG cybersecurity center, is working on the technical response for spam. As of 2022, no specific technical solutions have implemented for spam. However, The PNG government has a plan to implement technical solutions for spam prevention and it is on the planning stage.

2) Self-regulation

PNG doesn’t have anti-spam self-regulation scheme. However, they have a plan to create a new self-regulation scheme and it is on the planning stage. National Information and Communication Technology Act 2009 requires industry self-regulation through recognized association.

The PNG government responded that Under Cyber Crime Code Act, service providers are required to assist law enforcement in the prevention, or prosecution of an offence and to terminate or prevent action which would result in the commission or continuation of an offence relating ICT.

National Information and Communication Technology Act 2009

3. Regulatory Principles

To achieve the objective of this Act set out in Section 2, Parliament intends that the ICT industry in Papua New Guinea be regulated in a manner that recognizes –

(a) the effectiveness of market forces in promoting consumer welfare, specifically that –

(i) to the extent that markets are competitive, primary reliance should be placed on commercial negotiations and the greatest practicable use of industry self-regulation, subject to minimum regulatory requirements consistent with the objective of this Act;

3) Education/ Awareness raising

At present, Department of ICT and NICTA are conducting awareness raising through media. Also, PNG Computer Society and PNG Computer Emergency Response Team are working on online awareness. Department of Education needs to take a lead on this issue.

However, PNG doesn't have any private sector initiatives related to the education and awareness-raising on spam.

E. International cooperation

PNG doesn't participate in any international cooperation initiatives on spam. However, PNG has a plan to make an international cooperation initiative and it is in the stage of research. Also, they think information sharing related to spam is the challenge to counter spam effectively cross-border.

3.1.20. Philippines

A. Definition of spam

In Philippines, spam messages are unsolicited and unwanted commercial and promotional advertisement and surveys.

B. Current status for spam response

In case of Philippines, current status for spam response is not identified.

C. Legislation related to spam

1) Key concepts

Broadcast Messaging Service is messaging service that allows one to send the same SMS/MMS messages to many mobile phones.

Push messages are information transmitted to the mobile phone, either subscribed or unsolicited messages, without a user request and are initiated by the PTE (Public Telecommunications Entity) or CP (Content Provider).

Spam messages are unsolicited and unwanted commercial and promotional advertisement and surveys.

2) Contents of spam legislation

The Philippine government basically adopts opt-in scheme for spam messages (SMS, MMS), but there is no regulation on spam emails.

Although Philippines has not yet enacted comprehensive spam regulations, the National Telecommunications Commission (NTC) regulates broadcast messages by enacting enforcement rules and regulations on broadcast messaging services in accordance with the Act to Promote and Govern the Development of Philippine Telecommunications and the Delivery of Public Telecommunications Services (Public Telecommunication Services Act).

The rules create an opt-in mechanism for receiving unsolicited commercial messages sent by SMS or MMS. All such messages must identify the sender and provide sender contact details.

Here is the content of Rules and regulations on Broadcast messaging service.

1. 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.

2. All Content Providers shall register with Commission. All non-registered Content Providers shall, within fifteen (15) days from the date of effectivity of this Rules, register with the Commission.

3. All promos to be sent via broadcast/push messaging service shall be registered and approved by the Department of Trade and Industry (DTI), provided however that the DTI shall not approve promos of PTEs, and CPs not registered with the National Telecommunications Commission (NTC). The DTI shall furnish the NTC with the list of registered and approved promos of PTEs and CPs.

4. PTEs shall enter into an agreement only with CPs registered with the NTC.

5. Subscribers/recipients who do not reply to Broadcast/Push messages shall be considered to

have not opted-in and such broadcast shall be stopped.

6. 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.

7. 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.

8. Broadcast/Push messages shall not be sent between 9:00 PM to 7:00 AM except on paid subscription services.

9. 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. The PTEs shall furnish the Commission with a list of the assigned codes of their CPs.

10. 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.

11. Opting-in/Opting-out shall be free of charge.

12. There shall be an exclusion list for each PTE/CP which it will regularly update to ensure that subscribers in the list are not sent broadcast messages.

13. The PTEs and CPs shall regularly consolidate/update their respective list of subscribers who have opted-in/opted-out.

14. Content and/or information providers and/or PTEs shall provide a system that shall accept the universal keywords “STOP”, “END”, “CANCEL”, “UNSUBSCRIBE” and “QUIT”, whether lower case or uppercase or combination to opt-out.

15. Content and/or Information providers and/or PTEs shall keep records of the opt-in and opt-out requests from the time a user/subscriber initiates opt-in for tat least six months after the user has opted out of the content/service or until ordered by the Commission for records subject of complaints.

Meanwhile, the Cybercrime Prevention Act of 2005 created an opt-out system in relation to commercial electronic communications. Commercial electronic communications must include subscription and unsubscribe facility and must not contain information that intentionally disguises or misleads the origin of an electronic message in order to convince the recipient to read the message. The term “commercial electronic communications” is not defined, but it appears to include electronic messages (such as e-mail) intended to advertise or sell or offer

goods and services. Violators of this provision may face imprisonment or a fine between 100,000 pesos and 600,000 pesos.

Here is the content of Cybercrime Prevention Act related to spam.

(3) Unsolicited Commercial Communications. — The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:

(i) There is prior affirmative consent from the recipient; or

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(iii) The following conditions are present:

> (aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject. receipt of further commercial electronic messages (opt-out) from the same source;
>
> (bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and
>
> (cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

However, in 2014, the Philippine Supreme Court, while upholding other provisions of the Cybercrime Prevention Act, struck down as unconstitutional the provision on unsolicited commercial communications for violating a person's right to freedom of expression.[6] Therefore, there is currently no regulation on spam e-mails sent through computer systems.

3) Regulatory authority

National Telecommunications Commission (NTC) in charge of spam regulation.

4) Penalties

Rules and regulations on Broadcast Messaging Service stipulate that a person who sends an unsolicited commercial message without (1) the recipient's prior consent and (2) the recipient's opt-in shall be subject to appropriate administrative and penal punishment according to the regulation.

[6] https://www.linklaters.com/en/insights/data-protected/data-protected---philippines

1. Non-compliance and/or violation of any of the provisions of this rules and other relevant laws, rules and regulations of this Commission, shall subject the violator/respondent to cancellation or suspension of their provisional authority/certificate of public convenience and necessity (PTEs) or cancellation or suspension of their certificate of registration (CPs) and imposition of the appropriate fines and penalties after due notice and hearing.

2. PTEs and CPs in violation of this Rule shall be blacklisted by the Commission. Blacklisted PTEs and CPs shall not be allowed to engage in broadcast messaging services.

3. Violation of this Rule, notwithstanding the above provisions, shall subject the PTE/CP to a penalty of two hundred pesos (P200.00) per violation per subscriber.

4. Each text spam shall be considered as a violation. Also, every provision violated or not complied by the PTEs and CPs shall be considered as a violation.

5. PTEs/CPs violating the provisions of this Rule shall be subject to the following administrative fines and penalties:

- Twenty (20) violations or less (per quarter of every year); fines of P200 per violation

- More than twenty (20) violations to fifty (50) violations (per quarter of every year); fine of P200 per violation, blacklisting and suspension of provisional authority/certificate of public convenience and necessity (PTEs) or suspension of their certificate of registration (CPs)

- More than fifty (50) violations (per quarter of every year); fine of P200 per violation and cancellation of provisional authority/certificate of public convenience and necessity (PTEs) or cancellation of their certificate of registration (CPs)

D. Spam policy

In case of Philippines, spam policy is not identified.

E. International cooperation

Philippines signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.1.21. Singapore

A. Definition of spam

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.

Spam is unsolicited commercial electronic messages sent in bulk. Such messages could be sent via mobile telephony systems or electronic mail (e-mail). Spam typically advertises or promotes goods or services, land, business opportunities or investment opportunities.

B. Current status for spam response

Although spam transcends national boundaries, Singapore, as an information and communications technology hub, has put in place measures to keep it in check. Public education and technical countermeasures act as the first line of defense.

Spam control is challenging for a few key reasons. Its global nature means local measures will not be sufficient. It is challenging because spammers will find ways to outsmart technological means to control spam. Also, it is impossible to classify every spam as such since some recipients welcome them as a means of keeping tabs on offers and promotions in the market.

Nuisance calls encompass any type of unwanted, unsolicited telephone call. Common types of nuisance calls include prank calls, malicious calls, telemarketing calls and silent calls. Such cases may be referred to service providers for value added solutions to block or trace calls, or to the relevant authorities if the content is offensive or contains elements of threat.

The Personal Data Protection Commission (PDPC) regulates the sending of telemarketing messages under the Do Not Call (DNC) Provisions in Part IX of the Personal Data Protection Act 2012 (PDPA). The DNC Provisions generally prohibit organizations from sending certain unsolicited marketing messages (in the form of voice calls, fax, or text messages) to Singapore telephone numbers, including mobile, fixed-line, residential and business numbers, that are listed on the DNC Registry.

C. Legislation related to spam

1) Key concepts

"**Commercial electronic message**: an electronic message, where, having regard to -
(a) the content of the message;
(b) the way in which the message is presented; and
(c) the content that can be located using the links, telephone numbers or contact information (if any) set out in the message,

It is concluded that the primary purpose of the message is-

To offer to supply goods or services/ to advertise or promote goods or services/ to advertise or promote a supplier, or a prospective supplier, of goods or services/ to offer to supply land or an interest in land/ to advertise or promote a supplier, or a prospective supplier, of land or an interest in land/ to offer to provide a business opportunity or an investment opportunity/ to advertise or promote a business opportunity or an investment opportunity/ to advertise or promote a provider, of a business opportunity or an investment opportunity/ to assist or enable a person, by deception, to dishonestly obtain property belonging to another person/ to assist or enable a person, by deception, to dishonestly obtain a financial advantage from another person/ to assist or enable a person to dishonestly obtain a gain from another person..

"unsolicited"

An electronic message is unsolicited if the recipient did not (a) request to receive the message or (b) consent to the receipt of the message.

"Sending in bulk"

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;

"Singapore link"

This act shall not apply unless an electronic message has a Singapore link. An electronic message has a Singapore link in the following circumstances;

(a) the message originates in Singapore

(b) the sender of the message is an individual who is physically present in Singapore when the message is sent or an entity whose central management and control is in Singapore when the message is sent

(c) the computer, mobile telephone, server or device that is used to access the message is located in Singapore

(d) the recipient of the message is an individual who is physically present in Singapore when the message is accessed or an entity that carries on business or activities in Singapore when the message is accessed

(e) if the message cannot be delivered because the relevant electronic address has ceased to exist (assuming that the electronic address existed), it is reasonably likely that the message would have been accessed using a computer, mobile telephone, server or device located in Singapore.

“Dictionary attack”
The method by which the electronic the electronic address of a recipient is obtained using an automated means that generates possible electronic addresses by combining names, letters, numbers, punctuation marks or symbols into numerous permutations.

2) Contents of spam legislation

(1) Regulatory framework

Basically, the Singaporean government has an opt-out system for spam emails, spam messages and spam phone calls.

The Spam Control Act came into effect in June 2007 and created an opt-out mechanism for bulk commercial electronic messages with Singapore link. Email, SMS, and MMS messages fall within the scope of this system, and messages sent via fax or fixed phone numbers, voice calls are not included.

The definition of commercial electronic message is an electronic message with the purpose of (1) offering, advertising, or promoting the supply of goods and services, or (2) helping a person obtain property or financial gain by dishonest or deceitful means from another person. A commercial electronic message becomes unsolicited if the recipient does not (1) request receipt of the message or (2) consent to receipt of the message. This Act only applies to electronic messages with Singapore link. A Singapore link is created when an electronic message is created in Singapore or is created abroad and accessed in Singapore.

An electronic message is considered bulk if the same sender (defined as the person who sent, caused or authorized the sending of the message) sends:

- More than 100 messages with the same or similar subject in 24 hours
- More than 1000 messages with the same or similar subject in 30 days
- More than 10,000 messages with the same or similar subject in one year

Any person who sends unsolicited commercial electronic messages in bulk must comply with the requirements of the Spam Control Act.

(Application) Any person who sends, causes to be sent or authorizes the sending of unsolicited commercial electronic messages in bulk shall comply with the requirements in the Second Schedule.

(Unsubscribe facility) Every unsolicited commercial electronic message shall contain an electronic mail address, an Internet location address, a telephone number, a facsimile number or a postal address that the recipient may use to submit an unsubscribe request and a statement to the effect that the recipient may use the electronic mail address, Internet location address, telephone number, facsimile number or postal address, as the case may be, provided in the unsolicited commercial electronic message to submit an unsubscribe request, or a statement to similar effect.

(No further message shall be sent after unsubscribe request) Where a recipient submits an unsubscribe request using the facility provided pursuant to this paragraph, 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.

In addition to the above regulations under the Spam Control Act, there are the following Do-Not-Call registry regulations under the Personal Data Protection Act, which apply to voice calls, fax, and text massages.

(Duty to check register) a person must not send a specified message addressed to a Singapore telephone number unless the person has, at the time the person sends the specified message, valid confirmation that the Singapore telephone number is not listed in the relevant register.

(Contact information) a person must not send a specified message addressed to a Singapore telephone number unless the specified message includes clear and accurate information identifying the individual or organization that sent or authorized the sending of the specified message.

(Calling line identity not to be concealed) a person that makes a voice call containing a specified message or causes a voice call containing a specified message to be made or authorizes the making of a voice call containing a specified message, addressed to a Singapore telephone number, from a telephone number or fax number, must not do any of the following:

(a) conceal or withhold from the recipient the calling line identity of the sender;
(b) perform any operation or issue any instruction in connection with the sending of the specified message for the purpose of, or that has the effect of, concealing or withholding from the recipient the calling line identity of the sender.

(Consent) A person shall not, as a condition for supplying goods, services, land, interest or opportunity, require a subscriber or user of a Singapore telephone number to give consent for the sending of a specified message to that Singapore telephone number or any other Singapore telephone number beyond what is reasonable to provide the goods, services, land, interest or opportunity to that subscriber or user, and any consent given in such circumstance is not validly given.

(Withdrawal of consent) On giving notice, a subscriber or user of a Singapore telephone number may at any time withdraw any consent given to a person for the sending of any specified message to that Singapore telephone number.

(2) Labelling and other requirements

(Labelling) 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.

(Code of practice) Internet access service providers and telecommunications service providers may, with the approval of the Authority, issue a code of practice in connection with minimum standards of technical measures to effectively control the sending of unsolicited commercial electronic messages; and such other matters as the Authority may require.

(3) Regulation on address harvesting software

The Spam Control Act prohibits sending electronic messages to electronic addresses obtained or generated through the use of dictionary attacks or the use of address harvesting software, regardless of whether the messages are unsolicited or of a commercial nature.

(Use of dictionary attack and address harvesting software)

This shall apply to all electronic messages, whether 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 using (a) a dictionary attack or (b) address harvesting software.

The Personal Data Protection Act also has regulations that prohibit dictionary attacks and address harvesting software.

3) Regulatory authority

Responsibility for managing unsolicited communications falls to the Personal Data Protection Commission (PDPC), which was established to implement the PDPA, 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. The PDPC also has responsibility for personal data protection, 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, encompassing:

- the legislative framework (i.e. the Act);
- industry self-regulation – the three major Internet Service Providers (ISPs), under the facilitation of IMDA, have established spam control guidelines. These guidelines have been adopted jointly by the three ISPs to reduce e-mail spam for their subscribers. The Direct Marketing Association of Singapore (DMAS) has also launched an E-mail Marketing Code of Practice for its members;
- international cooperation, through participation in various networks to assist global efforts to curb spam; and
- public education – providing information for individuals and organizations on spam and how to combat it, including with the help of IMDA industry partners as appropriate. Consumers can also take direct action against an offender of the Spam Control Act through civil action.

4) Penalties

The statutory damages shall not exceed SGD 25 for each unlawful electronic message. Also, unless the litigants prove their actual loss due to the violation exceeds SGD 1 million, the maximum shall not exceed SGD 1 million.

(Statutory damages)

(i) not exceeding $25 for each electronic message referred to in section 13(1); and

(ii) not exceeding in the aggregate $1 million, unless the plaintiff proves that his actual loss from such electronic messages exceeds $1 million.

Civil action

The Spam Control Act grants the right of civil action to Internet service providers, e-mail service providers and individuals who suffer loss or damage as a direct or indirect result of a violation of the Act. These individuals or entities may bring civil action against (1) any person who sent, caused or authorized the sending of an electronic message, or (2) any person who aided, taught, or assisted in a violation of the Act. The types of relief that the court may grant an injunction or recovery of ordinary damages or recovery of statutory damages. The party to the litigation must choose between ordinary damages and statutory damages. They cannot choose both to recover.

D. Spam policy

1) Technical response

In case of Singapore, telecommunication service providers, are required to implement anti-spam measures such as blocking scam SMS/calls. The details of this technical response can be found in the following link.https://www.imda.gov.sg/-/media/Imda/Files/News-and-Events/Media-Room/Media-Releases/2022/08/Annex-A.pdf

2) Self-regulation

The three major Internet Service Providers (ISPs), under the facilitation of IMDA, have established spam control guidelines. These guidelines have been adopted jointly by the three ISPs to reduce e-mail spam for their subscribers. The Direct Marketing Association of Singapore (DMAS) has also launched an E-mail Marketing Code of Practice for its members.

3) Education/ Awareness raising

IMDA provides public education providing information for individuals and organizations on spam and how to combat it, including with the help of IMDA industry partners as appropriate. Also, PDPC is providing information on how to protect their citizens from the spam and scam.

E. International cooperation

Singapore didn't join UCENet. However, Singapore signed the Regional Comprehensive Economic Partnership (RCEP) agreement. Also, IMDA and ACMA signed Memorandum of Understanding for enhanced cooperation to combat scam and spam communications. The MOU was signed on 18 July 2022.

This MOU has been developed in connection with the Australia-Singapore Digital Economy Agreement, as well as the Joint Declaration by the Prime Ministers of Australia and Singapore on a Comprehensive Strategic Partnership's objective to deepen bilateral relations and cooperation and enhance the integration of the economies of Australia and Singapore.

The MOU covers cooperation in key areas such as information sharing and assistance in investigations relating to scam and spam calls and short message services. Parties have also agreed to mutual exchanges of knowledge and expertise and collaboration on technical and commercially viable solutions in relation to such scam and spam communications' sees cooperation from less developed countries that lack resources to combat spam/scam as challenges to counter spam effectively cross-border.

3.1.22. Sri Lanka

A. Definition of spam

Sri Lanka does not possess a national law or regulation pertaining to spam and it is not defined under any law or regulation. Sri Lanka is currently in the process of defining spam. The National Minimum Information Security Standards of Sri Lanka stresses the importance of safeguarding the email servers through the restrictions of spam.

B. Current status for spam response

At the organizational level, spam messages are restricted through the use of spam filters and other related technologies. If governments receive a complaint from a telecom subscriber, government will forward it to relevant operator for necessary action.

Currently there is no mechanism to track and monitor the statistics for spam at National level and also there is no specific reporting system for SPAM messages. In addition, Sri Lanka does not have a mechanism to identify SPAM messages or their source and routes of SPAM traffic. However, there is a dedicated email address to report SCAM alerts.

Sri Lanka has issues related to spam legislation, technical issues, law enforcement and international cooperation. There is a lack of legislations and national level policies governing

the management of spam. Furthermore, there are a lack of technologies to control spam at a national level. Currently these issues are being identified and addressed. Due to the growth in usage of digital devices, issues related to spam are being highlighted now and the corrective measures will be taken in the near future.

In Sri Lanka, mainly telecommunication service providers are engaged in anti-spam activities. Telecommunication operators use spam filtering mechanisms to filter out spam messages based on set of spam patterns. At organizational level, spam filters are implemented.

C. Legislation related to spam

There is no general anti-spam act, but the government of Sri Lanka believe they need the general anti-spam law and has plan to legislate one. They are still in the stage of planning but expect to have a general anti-spam law in 1-2 years.

D. Spam policy

1) Technical response

There are no technical solutions implemented by the government, but these are being carried out at organizational level. Telecommunication operators use spam filtering mechanisms to filter out spam messages based on set of spam patterns. At organizational level, spam filters are implemented. However, the government of Sri Lanka has a plan to implement technical solutions at the country level and they are in the stage of planning. They are worrying about the lack of resources (information, experts, funds, etc.) preparing technical solutions.

2) Self-regulation

There is no anti-spam self-regulation scheme in Sri Lanka. However, Sri Lanka has a plan to create self-regulation scheme. They are worrying about the lack of resources (information, experts, funds, etc.).

3) Education/ Awareness raising

There is no anti-spam policy related to the education and awareness-raising on spam in Sri Lanka. However, education and awareness raising through social media pages of government organizations have been conducted and SMS have been sent to subscribers by telecommunication operators from time to time.

Sri Lanka does not have a plan to create education and awareness-raising policy because of the lack of resources (information, experts, funds, etc.).

E. International cooperation

Sri Lanka doesn't participate in any international cooperation initiatives on spam due to the lack of resources (information, experts, funds, etc.). However, Sri Lanka has a plan to make an international cooperation initiative and it is in the stage of planning. However, they don't have plans to join any existing international cooperation initiatives. Also, they think cross border coordination and technical solutions related to spam are the challenges to counter spam effectively cross-border.

3.1.23. Thailand

A. Definition of spam

Spam is defined as 'a computer data or an electronic mail to another person while hiding or faking its sources, in a manner that interferes with such another person's normal utilization of the computer system'. (COMPUTER-RELATED CRIME ACT, 2007)

All of electronic data that do not comply with the Notification of the Ministry of Digital Economy and Society regarding the characteristics and method of sending, characteristics and size of data, and frequency and method of sending, is Spam.

B. Current status for spam response

In the case of Thailand, survey result shows that there are issues related to the current technical aspect, government-private cooperation, law enforcement, international cooperation, and awareness raising regarding spam. Therefore, when APT provides programs to enhance the capacity of member countries, Thailand responded that programs such as education for government officials, policy consulting through the APT Expert Mission, and on-the-job training are needed. In the case of training, 1) an overall overview of the anti-spam legal system, 2) global norms and trends, 3) analysis of current regulations and problems of each APT member country, and 4) interactive workshops on solutions are particularly necessary. And, Thailand answered that the main target of the training should be the deputy director level or manager level working group in charge of spam-related issues.

In the case of policy consulting, they answered that they need information sharing and on-the-job training from experts dispatched by APT the most.

In Thailand, it was found that the government and telecommunication service providers are mainly engaging in anti-spam activities, and industry associations and non-governmental organizations are not so actively engaging. Telecommunication service providers are mainly responding to spam by using their own spam filtering technology.

C. Legislation related to spam

1) Key concepts

There is no comprehensive anti-spam legislation in Thailand. However, it is an offence under the Computer Crime Act to send emails and data with concealed information as to their source in such a way that interferes with the normal operation of the recipient's computer system (maximum penalty: THB100,000 fine (approximately USD$3,100)). This offence could apply to sending a spam message in some circumstances.

In addition, followings are included in spam messages:

- false data that is likely to undermine national security or cause public unrest; or
- forged data that is likely to cause damage to a third party or to the public

It will be an offence under the Computer Crime Act to disseminate these messages through a computer system.

2) Contents of spam legislation

The Thai government basically applies an opt-in system to spam e-mails. The Computer Crimes Act provides the followings.

(Prohibit electronic mail that interferes normal utilization of computer system) Whoever sends computer data or an electronic mail to another person while hiding or faking its sources, in a manner that interferes with such another person's normal utilization of the computer system, shall be liable to a fine not exceeding One Hundred Thousand Baht.

(Prohibit electronic mail that doesn't have unsubscribe facility) Whoever sends computer data or electronic mail to another person in a manner that disturbs the recipient, without giving

the recipient an easy opportunity to cancel or notify his/her wish to deny receipt of such computer data or electronic mails, shall be liable to a fine not exceeding Two Hundred Thousand Baht.

In the case of spam, the sender must offer an easily accessible method to opt out, so recipients can refuse to receive future emails.

(Prescribe the characteristic and method of sending electronic mail by Minister) The Minister shall prescribe and announce the characteristic and method of sending computer data or electronic mail, including the characteristic and size of the computer data or electronic mail which shall not be considered as disturbing the recipient, as well as the manner in which the recipient can easily cancel or notify his/her wish to deny receipt of such computer data or electronic mails.

According to this provision of the act, the MDES issued a notification[7] that sets out the characteristics and methods of sending emails and data, and characteristics of computer data or emails that are not considered to cause a disturbance to the recipient. This notification acts as a set of "safe-harbor rules" for business operators when sending emails to customers, prospective customers, or even to business partners or third parties.

The following types of emails and data are assumed not to cause a disturbance to the recipient if they are:

- Sent to another person as evidence of an agreed contractual transaction, or for compliance with law, or for expressing a relationship or a legal relationship between each other.
- Sent by a government body that enforces the law, for the purpose of providing communications that are not for commercial purposes.
- Sent by an educational institution, a charitable body, or other organizations, which is not for commercial purposes.
- Sent in a legal manner that does not violate any individual rights and which is not for commercial purposes.

The notification states that emails and data for commercial purposes (and not within the scope of the four examples above) are only permissible when consent has been obtained from the recipient, and the following conditions are met:

Emails and data must specify the signs, details, and processes that will enable the recipient to opt out of or unsubscribe from receiving such emails, including technical measures allowing

[7] https://www.bangkokpost.com/business/1428591/computer-crimes-act-and-spam

the recipient to do so quickly.

After a request to unsubscribe has been made, the sender must suspend the sending of emails and data to the recipient immediately or, in certain circumstances, within seven days from the receipt of the request.

It is strictly prohibited for the process or request form for opting out/unsubscribing to be conditional or to divert for any additional commercial purposes (for example, if clicking the opt-out request routes the user to other websites or other sales distribution channels).

If the sender continues to send emails and data to the recipient after a request has been made, the recipient may send another request, in writing, by way of an email, registered mail with return receipt, or any other way by which they can confirm receipt. If the sender continues to send emails and data after receiving a request of this nature, the sender is deemed to be committing the spam offence under Section 11 of the Computer Crime Act.

3) Regulatory authority

Ministry of Digital Economy and Society (MDES) and National Broadcasting and Telecommunications Commission (NBTC) are in charge of spam regulation.

4) Penalties

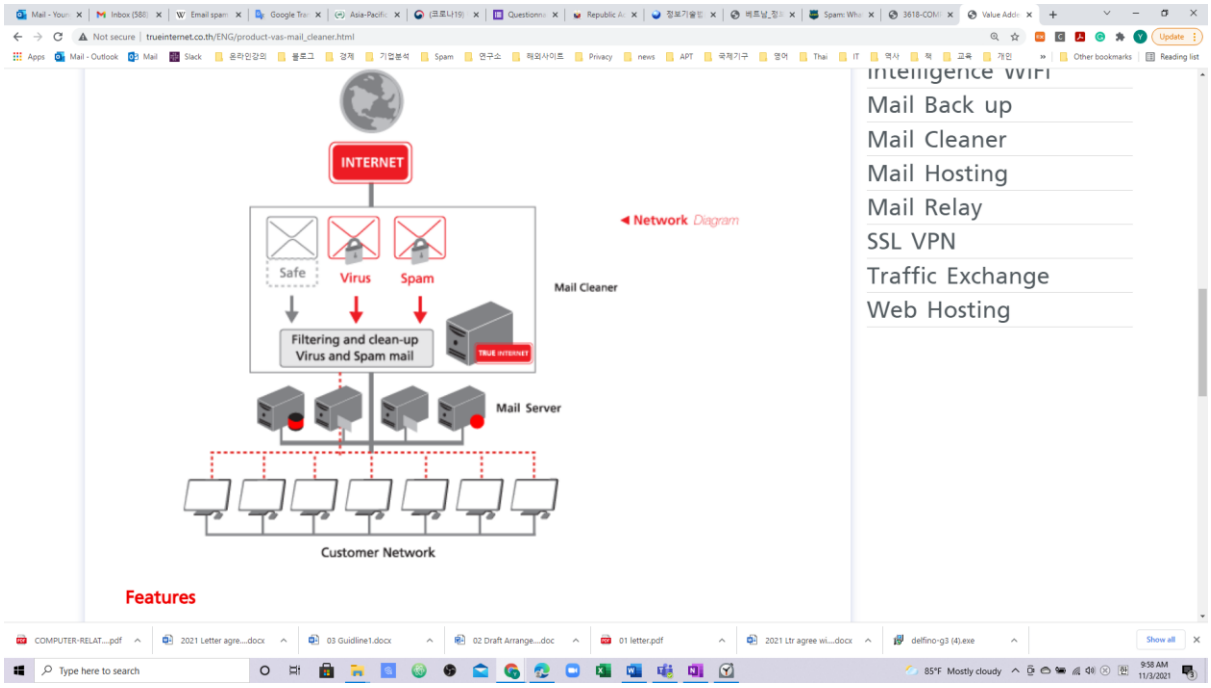
This spam email and data offence could attract a maximum fine of 200,000 baht per spam communication.

4. Spam policy

1) Technical response

In the case of Thailand, it was found that True Internet (Internet service provider) provides a technical solution called 'Mail Cleaner'. To optimize corporate server performance, Mail Cleaner ensures the server is clean and clear from viruses and spam. Mail Cleaner filters and scans all incoming emails to prevent spam and any possible virus. Once detected, the system then eliminates them before sending the mails to the user's mail server. Mail Cleaner usually makes an update on a daily basis to ensure the utmost protection.

< Structure of Mail Cleaner system >



Features

- Suitable for organizations having their own mail servers
- No additional installation and maintenance of server based anti-spam and anti-virus systems
- A comprehensive anti-spam and anti-virus solution
- If the server is down or temporarily unreachable, the emails will be queued for three days for future delivery.

2) Self-regulation

Thailand has anti-spam self-regulation scheme (self-regulation mechanism developed and operated by service providers, industry associations, and non-governmental organizations.) Thailand introduced that Code of Practice was developed by a private mail marketing company "Get response".

3) Education/ Awareness raising

At present, it has been confirmed that there is no policy related to education or awareness raising on spam in Thailand. And it was found that this was due to the lack of manpower or financial resources for the policy. Also, Thailand confirmed that there is no education and

awareness-raising activities in the private sector.

E. International cooperation

It was confirmed that Thailand is not currently participating in international cooperation initiatives related to spam and has no plans to create such an international cooperation initiative. And it was found that this was due to the lack of manpower or financial resources for the policy. However, Thailand signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

Also, the Thai government recognized that solving the problem of SMS spam from other countries is a major challenge in relation to the cross-border spam problem.

3.1.24. Tonga

A. Definition of spam

In case of Tonga, they don't have any definition of spam on regulation. However, the international technical definition of spam remains active.

B. Current status for spam response

In Tonga, government doesn't have any reporting system, so they aren't measuring spam from the government side. However, they noticed that spam emails can cost in the mis-utilization of the network bandwidth.

In the case of Tonga, survey result shows that there are issues related to the legislation, technical aspect, international cooperation regarding spam. They answered that email spams are still a big challenge since it is not affordable for many people in Tonga to have genuine office tools especially MS Office. It allows spam injections as cracked version have less security.

Therefore, when APT provides programs to enhance the capacity of member countries, Tonga responded that programs such as training to government officials, policy consulting through the APT Expert Mission are needed. In the case of training, 1) an overall overview of the anti-spam legal system, 2) global norms and trends, 3) specific rules and regulations, 4) analysis of current regulations and problems of each APT member country, 5) best practices, recent development, etc., and 6) interactive workshops on solutions are particularly necessary. And Tonga answered that the main target of the training should be the director level, deputy director and manager level government officers in charge of spam-related issues.

In the case of policy consulting, they answered that they need information sharing, drafting new anti-spam act, and drafting strategic plan for anti-spam from experts dispatched by APT the most.

C. Legislation related to spam

1) Key concepts

There is no comprehensive anti-spam legislation in Tonga. So, they don't have any definition of spam on regulation.

2) Contents of spam legislation

There is no comprehensive anti-spam legislation in Tonga and currently they don't have any plan to legislate new act. However, Tonga administration wishes to get a support from APT to legislate an act for spam.

3) Regulatory authority

Both the Ministry of Meteorology, Energy, Information, Disaster management, Environment, Climate Change and Communications (MEIDECC) and CERT Tonga are cooperating each other in terms of spam response. However, currently CERT Tonga has very little action on spam issue.

4) Penalties

There is no comprehensive anti-spam legislation in Tonga. So, they don't have any regulation on spam penalties.

4. Spam policy

1) Technical response

In the case of Tonga, it was found that government doesn't have any specific technical solutions on spam issue and survey shows that it is because the lack of resources (information, experts, fund, etc.)

2) Self-regulation

Tonga doesn't have anti-spam self-regulation scheme and survey shows that it is because the lack of resources (information, experts, fund, etc.).

3) Education/ Awareness raising

At present, Tonga doesn't have any education/ awareness raising programs and survey shows that it is because the lack of resources (information, experts, fund, etc.).

E. International cooperation

According to the survey, Tonga hasn't joined any international cooperation initiatives and survey shows that it is because the lack of resources (information, experts, fund, etc.).

3.1.25. Viet Nam

A. Definition of spam

Although Vietnam's law on spam, Law on Information Technology, does not specifically define spam, the enforcement decree does specify the definition of spam. Enforcement Decree 91 separates spam messages, e-mails, and telephone calls, and the definitions are as follows.

Spam messages include:

a) Advertising messages that are sent without users' prior consent or advertising messages that violate the regulations of this Decree on sending advertising messages;

b) Messages that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

Spam emails include:

a) Advertising emails that are sent without users' prior consent or advertising emails that violate the regulations of this Decree on sending advertising emails;

b) Emails that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

Spam calls include:

a) Advertising calls that are made without users' prior consent or advertising calls that violate the regulations of this Decree on making advertising calls;

b) Calls that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

B. Current status for spam response

The Vietnamese government has recently been intensively responding to the robocall problem and launched a spam portal service to respond to spam emails and spam messages.[8]

In the first half of 2021, mobile carriers blocked more than 92,000 subscribers from spreading spam calls and stopped over 35 million fake calls.

In recent years, Vietnam has recorded increasing numbers of fake calls and spam calls. A new form of automatic advertising call (robocall) has appeared.

In July 2020, the Ministry of Information and Communications asked network operators to take

[8] https://vietnamnet.vn/en/sci-tech-environment/vietnam-wins-big-in-the-battle-against-scam-spam-calls-759248.html

https://vietnamnews.vn/economy/1086539/portal-on-preventing-and-combating-spam-launched.html

measures to prevent fake and spam calls. By the end of June 2021, local network operators blocked more than 181,000 subscribers from spreading spam calls.

The number of people's complaints about spam calls over the number 5656 has increased by an average of 13-15%/month. This shows people's interest and response to measures to prevent spam calls.

A representative of the Department of Telecommunications said that the number of spam calls and the number of affected subscribers has decreased significantly. In June 2021, there were about 8.4 million spam calls, down 31.9% compared to December 2020 with more than 5.4 million subscribers affected, down 23.5% compared to December 2020.

The Department of Telecommunications has instructed network operators to build a system to detect and prevent fake calls. By the end of June 2021, Vietnamese telecom service providers prevented more than 56.65 million fake calls.

In November 2021, the Authority of Information Security (Ministry of Information and Communications, MIC) officially put into operation a portal to prevent and combat spam messages and spam emails at http://chongthurac.vn.

Thus, in addition to sending a notification message about the phone number spreading spam to the hotline 5656, from now on, individuals and organizations can look up their identifiers online through the portal chongthurac.vn.

Previously, the Authority of Security Department allowed organizations and individuals to search through SMS messages. Currently, individuals and organizations can look up identifiers on the portal.

The addition of the identifier name lookup function on the website is a prominent new feature, helping organizations and individuals easily look up online identifiers issued by the Authority of Information Security or declared by telecommunications carriers.

The portal also posts instructions and information on spam messages, phishing messages, spam calls, scam calls, spam emails; inspection, examination and sanctioning activities and technology solutions related to the prevention, combat and blocking of spam messages, spam emails and spam calls.

Along with linking to the non-advertising list management system and guiding people to register or unsubscribe from the non-advertising list, the Viet Nam Computer Emergency Response Team (VNCERT) will also update and publish a list of IP addresses and IP range spreading spam messages on the portal.

C. Legislation related to spam

Vietnam has a fairly comprehensive spam regulation, as the Enforcement Decree 91 of the Law

on Information Technology (Fighting Spam Messages, Span Emails and Spam Calls) contains detailed provisions for resolving spam.

1) Key concepts

Spam messages include:

a) Advertising messages that are sent without users' prior consent or advertising messages that violate the regulations of this Decree on sending advertising messages;

b) Messages that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

Spam emails include:

a) Advertising emails that are sent without users' prior consent or advertising emails that violate the regulations of this Decree on sending advertising emails;

b) Emails that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

Spam calls include:

a) Advertising calls that are made without users' prior consent or advertising calls that violate the regulations of this Decree on making advertising calls;

b) Calls that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

Regulated entities

Decree 91 applies to organizations and individuals involved in the fight against spam messages, spam emails and spam calls; the sending of advertising messages, emails and making of advertising calls in Vietnam, including:

- Providers of telecommunications services and/or Internet services.
- Organization establishing private telecommunications networks.
- Enterprises and organizations providing emailing services.
- Senders of advertising messages, emails, and calls (hereinafter referred to as "advertises")
- Recipients of advertising messages, emails, and calls (hereinafter referred to as "users")
- Relevant organizations and individuals.

2) Contents of spam legislation

(1) Regulatory framework

Basically, the Vietnamese government has an opt-in system for spam emails, messages, and phone calls. Article 70 of the IT Law includes three articles under the title of prevention of spam. Paragraph 1 states that when an individual or organization sends information over a network, that person or organization shall not hide their name or impersonate another organization or individual. Although the purpose of this provision may be seen to be to ensure that spammers can properly identify themselves, this prohibition in Article 70(1) is not limited to spam, and it can be applied to all information (such as emails, online posts, information submitted using online forms) transmitted through the network.

The second clause stipulates that when advertisement information is sent over a network, it must include an unsubscribe facility. There is no limit to the scope of this requirement, but it applies to all advertisement information (even though this term is not defined in the law).

Finally, Article 70(3) provides that a sender must stop sending this information to an individual when an individual notifies the sender that they no longer want to receive advertisement information.

Article 70.- Prevention of spam

1. When sending information in the network environment, organizations and individuals may not hide their names or impersonate other organizations or individuals.

2. Organizations and individuals that send advertisement information in the network environment shall assure consumers' ability to reject the advertisement information.

3. Organizations and individuals may not continue sending advertisement information in the network environment to consumers if the latter notify their refusal to receive the advertisement information.

In more detail, the Enforcement Decree stipulates definitions of spam-related terms, measures taken by stakeholders to prevent spam, Do-Not-Call Register, regulations on spam, reporting, and administrative penalties.

Decree 90/2008 used to only impose restrictions on marketing text messages and e-mail (but not telephone). However, Decree 91/202 now introduces a range of new restrictions on telemarketing activities and corresponding sanctions.

The main regulations are as follows.

(Rules for sending advertising messages, emails and making advertising calls)

1. 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.

2. Advertisers may only send only one unsolicited text message to a recipient without his/her consent, which is for purpose of soliciting consent, to a phone number that is not on the Do-Not-Call Register. The Ministry of Information and Communications shall elaborate regulations on sending opt-in messages.

3. In case the user refuses to receive advertisements or does not answer the only one unsolicited text message, the advertiser must not send any additional opt-in message or advertising message to that number.

4. Stop sending advertising messages and advertising emails and making advertising calls to the user after receiving the user’s unsubscribing request.

5. Each advertiser may send up to 3 advertising messages to a phone number, up to 3 advertising emails to an email address, and make 1 advertising call to a phone number within 24 hours unless otherwise agreed by the user.

6. Advertising messages may only be sent during 07:00 – 22:00; advertising calls may only be made during 08:00 – 17:00 unless otherwise agreed by the user.

7. Advertisement contents shall be conformable with advertising laws.

8. Only send advertising messages or make advertising calls after a brandname is issued;

Decree 91 introduces a "National Brandname Management System", which is intended to be used to manage and store brandnames worldwide and is developed and operated by the Authority of Information Security ("AIS") (under MIC). This system forms part of the State's effort towards combating spammers that replicate or hold themselves out as representatives of official brands (copycats). This system allows organizations and individuals to register the brandnames that would be used for advertising via messages or calls. Advertisers may only send advertising messages or make advertising calls after they have registered their brandname. Similar to IP registration, as brandname registration is done on a "first come first served" basis, organizations/individuals are encouraged to carry out registration as soon as possible to facilitate future marketing efforts. This may be done by post or electronically. Note that registration would require submission of, among others, documents proving usage of IP rights (e.g., trademark registration certificate). Brandname holders are subject to annual or ad hoc reporting to AIS, which includes matters such as revenue and growth metrics in connection with the brandname and the extent of advertising messages and calls used.

(Consent Requirements)

Decree 91 now specifies the method by which consent is to be obtained prior to sending advertising messages/emails/calls (the previous decree generally just required prior consent). Particularly, the recipient would need to give consent through either of the following methods:

(a) for advertising messages, agreeing to receiving such messages after the advertiser sends the first and only opt-in message (i.e.,) (b) declaring and completing a registration form on paper, website/portal, online application, or social network of the advertiser; (c) calling or sending a message to the advertiser's call center to subscribe; or (d) using a software program to subscribe.

(Option to unsubscribe from advertising messages)

1. The user's option to unsubscribe from advertising messages shall be clearly displayed at the end of the advertising message; instruct the user to unsubscribe from advertising messages to which the user previously subscribed; allow the user to reject a specific product or group of products where necessary; and contain clear instructions on how to unsubscribe.

2. The unsubscribing request can be made by sending a message; or making a call.

3. Right after the user's unsubscribing request, the advertiser shall send a confirmation and stop sending the refused type of advertising messages to the user.

4. The confirmation shall clearly state that the unsubscribing request has been received, time of receipt of the request and stopping sending advertising messages; be successfully sent once and not contain any advertisement.

(2) Labeling

(Advertising message requirements)

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.

3. Recipients have the option to refuse.

(Advertising email requirements)

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.

5. Recipients have the unsubscribing option.

(Option to unsubscribe from advertising emails)

1. The user's option to unsubscribe advertising emails shall be clearly displayed at the end of the advertising email; contains the statement that the user is entitled to refuse all products from the advertiser; allow the user to reject a specific product or group of products where necessary; and contain clear instructions to unsubscribe.

2. The unsubscribing request can be made by submitting a request on the website, web portal or social network; sending an email; or making a call.

3. Right after the user's unsubscribing request is received, the advertiser shall send a

confirmation and stop sending the unsubscribed advertising emails to the user.

4. The confirmation shall clearly state that the unsubscribing request has been received, time of receipt and stopping sending advertising emails; be successfully sent once and not contain any advertisement.

(Advertising call requirements)

1. All advertising calls shall contain adequate information about the caller (name and address) which is provide before the advertisement contents. Charges shall be specified if charged services are advertised.

2. If the user refuses to receive advertising calls, the advertiser shall promptly stop calling the user.

(3) Other regulation

(Do-Not-Call Registry and IP Blacklist)

Decree 91 introduces a "Do-Not-Call" registry and IP blacklist developed and operated by AIS. (a) Do-Not-Call Registry: This a compilation of phone numbers of persons who have registered not to accept any advertising calls or messages. Organizations and individuals that use telecommunications services will be able to register this list and withdraw from the same.

This list will be public. As such, advertisers will have an obligation to check the list to avoid making advertising calls or sending advertising messages to those numbers. Administrative fines of up to VND 100,000,000 may be imposed on organizations that send advertising messages or make advertising calls to numbers that are on this Do-Not-Call Registry. (b) IP Blacklist: This a list maintained by MIC which contains the IP addresses/domains that have been flagged as engaging in spam. It is periodically updated by MIC The list will be public, and organizations, enterprises and individuals may use this blacklist to block spam emails.

3) Regulatory authority

The Ministry of Information and Communications (MIC) is in charge of spam regulation.

4) Penalties

Along with the penalties listed in Decree 15/2020 (on penalties for violations of regulations on postal services, telecommunications, radio frequencies, information technology and electronic

transactions), stricter penalties are now applicable to violations of anti-spam regulations.

- Fines ranging from VND 5m to VND 10m will apply to the following violations: Making advertising calls to users without their clear prior consent; Making advertising calls to users who have unsubscribed to advertising calls; Sending opt-in message after the user has refused or does not response.

- Fines ranging from VND 20m to VND 30m will apply to the following violations: Making more than 1 advertising call to 1 phone number within 24 hours unless otherwise agreed by the user; Making advertising calls outside the 08:00 – 17:00 period unless otherwise agreed by the user; Failure to verify users' prior consents when sending advertising messages, advertising emails or making advertising calls; Failure to provide users with tools to access or retain agreements on subscribing and unsubscribing from advertising calls and opt-in messages on the website/web portal to facilitate inspection and complaint settlement.

- Fines ranging from VND 60m to VND 80m will apply to the following violations: Sending opt-in messages against regulations of the Ministry of Information and Communications; Sending an opt-in message to any phone number on the Do-Not-Call Register.

- Fines ranging between VND80m and VND100m will apply to advertisers who send any advertising text message or make any advertising phone call to a user/recipient of the 'Do-Not-Call' List.

- Fines ranging between VND10m and VND170m will also apply to violations committed by telecom/internet service providers, such as failure to provide tools or applications enabling users/recipients to proactively block spam emails or to report spam emails; failure to take measures to prevent advertising text messages/phone calls to users/recipients on the 'Do-Not-Call' List; or failure to take other professional measures when requested by the Information Security Department - Ministry of Information and Communications.

D. Spam Policy

The Authority of Information Security (Ministry of Information and Communications) officially put into operation a portal to prevent and combat spam messages and spam emails at http://chongthurac.vn. However, other spam policies in Viet Nam are not identified.

E. International cooperation

Viet Nam signed the Regional Comprehensive Economic Partnership (RCEP) agreement.

3.2. Comparative analysis and policy implications

3.2.1. Comparative analysis on legislation related to spam

A. Regulating Unsolicited emails

Member	Scheme	Consent required to email	Provide Sender information	Unsubscribe facility	Labeling obligation	Prohibit Address harvesting SW	Authority
Australia	Opt-in	yes	yes	yes	no	yes	ACMA
Korea	Opt-in	yes	yes	yes	yes	yes	KCC
Japan	Opt-in	yes	yes	yes	yes	yes	MIC
Singapore *	Opt-out	no	yes	yes	yes	yes	IMDA PDPC
China	Opt-in	yes	yes	yes	yes	yes	MIIT
Cook Islands	Opt-in	yes	yes	yes	no	yes	Office of the PM
Lao PDR	Lao PDR does not have specific regulation on unsolicited emails.						
Malaysia	Malaysia does not have specific regulation on unsolicited emails.						
New Zealand	Opt-in	yes	yes	yes	no	yes	DIA
Hong Kong	Opt-out	no	yes	yes	yes	yes	OFCA
India	India does not have specific regulation on unsolicited emails.						
Indonesia	Indonesia does not have specific regulation on unsolicited emails.						
Thailand	Opt-in	yes	no	yes	no	no	MDES NBTC
Pakistan	Opt-in	yes	no	yes	no	no	PTA
Papua New Guinea	N/A	N/A	no	no	no	no	NICTA
Philippines	Philippines does not have specific regulation on unsolicited emails.						
Viet Nam	Opt-in	yes	yes	yes	yes	no	MIC
Bhutan	Opt-out	no	yes	yes	no	no	MIC
Brunei	Brunei does not have specific regulation on unsolicited emails.						
Cambodia	Cambodia does not have specific regulation on unsolicited emails.						
Micronesi	Micronesia does not have specific regulation on unsolicited emails.						

a	
Nepal	Nepal does not have specific regulation on unsolicited emails.
Kiribati	Kiribati does not have specific regulation on unsolicited emails.
Sri Lanka	Sri Lanka does not have specific regulation on unsolicited emails.
Tonga	Tonga does not have specific regulation on unsolicited emails.

*In Singapore, only bulk emails and messages are regulated.

Regarding the regulation on spam e-mail, 9 of the 25 countries studied this year (Australia, Cook Islands, Republic of Korea, Japan, Singapore, P.R.China, New Zealand, Hong Kong, Viet Nam) have a comprehensive spam legislation. These countries are controlling spam by adopting an opt-in scheme (Australia, Cook Islands, Republic of Korea, Japan, P.R.China, New Zealand, Vietnam) or opt-out scheme (Singapore, Hong Kong). Regardless of the scheme, systematic regulatory framework to protect users from spam is established in these 9 countries. Australia, Cook Islands, Japan, Singapore, New Zealand, and Hong Kong have enacted separate spam laws. Republic of Korea, although not an individual spam law, has a separate section on spam in the Information and Communications Network Act and regulates spam specifically/systematically. P.R.China has established separate administrative regulations for spam, and Viet Nam has enacted enforcement Decree to comprehensively regulate spam emails.

In the case of Thailand, Pakistan, and Bhutan, unlike the above countries, there is no comprehensive legal system for spam e-mail, instead other laws regulate spam e-mails. Thailand has an opt-in system by stipulating that the Computer Crimes Act prohibits sending e-mails that interfere with the normal utilization of computer systems and prohibits sending e-mails without an unsubscribe facility. Pakistan also has an opt-in system by stipulating that the Electronic Crimes Act prohibits sending e-mails without permission and without an unsubscribe facility. PNG regulates spam based on Cybercrime Code Act. In the case of Bhutan, an opt-out system for spam e-mail regulation was created in the Information and Communication Media Act.

Cambodia, Lao PDR, Malaysia, Nepal, India, Indonesia, Philippines, Brunei, Micronesia, Kiribati, Tonga and Sri Lanka do not have direct and specific law or enforcement decree or administrative regulations on spam emails. However, these countries are also divided into Sri Lanka, Brunei, Micronesia (Federated States of) and Philippines, which do not regulate spam e-mails, and Malaysia, Indonesia, and Kiribati, which indirectly regulate spam e-mails to a certain level, although there are no direct regulations.

Malaysia does not have direct regulations against spam emails, but 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 a violation of the law. Of course, as discussed above, this regulation has limitations, but Malaysia is trying to regulate some of the spam emails.

Indonesia also does not have direct regulations on spam e-mail, 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." So, they are also trying to regulate some of the spam emails.

In the case of Kiribati, there are no direct regulations on spam emails. However, the Cybercrime Act 2021 covers in principle the nature of spam relating to unauthorized computer system access or unauthorized computer system interference should the spam carry a malicious payload to a computer system, interfering with its normal operation.

The Philippines originally had an opt-out regulatory system regulating unsolicited commercial electronic communications (e-mail, etc.) in the Cybercrime Prevention Act, but as the provision was determined to be unconstitutional, so there is currently no regulation on spam e-mails.

The similarities and differences are as follows, focusing on countries that have comprehensive regulatory framework for spam e-mails.

1) Similarities

Whether the statute adopted an opt-in scheme or an opt-out scheme, the core regulations were found to be similar.

(1) Provide accurate sender information

Countries with comprehensive spam control framework, whether adopting the opt-in method or the opt-out method, have in common that the sender provides accurate sender information to the recipient. Of course, 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.

Country	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)

(2) Provide unsubscribe facility

Countries with comprehensive spam control framework, whether adopting the opt-in method or the opt-out method, have in common that the sender provides the receiver with an unsubscribe facility. There are many cases where the unsubscribe facility is basically an e-mail address, but there are cases where specific means are not specified.

Country	**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

2) Differences

(1) Prior consent of recipient

In the case of countries adopting the opt-in system (Australia, Korea, Japan, China, New Zealand, and Vietnam), it is stipulated that prior consent must be obtained due to the nature of opt-in. In the case of opt-out (Singapore, Hong Kong), e-mails can be sent without prior consent. However, if the recipient notifies of their intention to reject the e-mail after receiving the e-mail, the sending of additional e-mails will be stopped.

Country	Prior consent
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.
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
Singapore	No
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;
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.
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

Hong Kong	No
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.

(2) Labeling obligation

Most countries with comprehensive anti-spam legislation have labeling obligations. In the case of labeling, it is easier for users to check whether it is an advertisement mail or not, and it is an effective regulatory measure because the burden on the sender due to labeling is not so large. However, whether or not the labeling obligation is applied in a country should be reviewed in consideration of the various situations and circumstances of the country concerned.

Country	Labeling obligation
Australia	No
Cook Islands	No
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.
New Zealand	No
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.

(3) Regulation on address harvesting software

Most countries with comprehensive anti-spam laws regulate address-harvesting software. Address harvesting software maximizes the damage of spam by allowing spam e-mail senders to easily send a large amount of e-mail to recipients, so it is desirable to be regulated and effective in enhancing user convenience. However, whether or not the address harvesting software is regulated, the necessity should be reviewed in consideration of the various situations and environments of the country concerned.

Country	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;
Viet Nam	No

(4) Bulk requirement

Unlike other countries, Singapore is subject to regulate spam only if it meets the requirement for sending emails in bulk. For other countries, there are no such bulk requirement.

Country	Bulk requirement
Australia	No
Republic of Korea	No
Japan	No
Singapore	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;
P.R.China	No
Cook Islands	No
New Zealand	No
Hong Kong	No
Viet Nam	No

B. Regulating Unsolicited SMS/MMS

Member	Scheme	Consent required to send message	Provide Sender information	Unsubscribe facility	Labeling obligation	Authority
Australia	Opt-in	yes	yes	yes	no	ACMA
Republic of Korea	Opt-in	yes	yes	yes	no	KCC
Japan	Opt-in	yes	yes	yes	yes	MIC
Singapore *	Opt-out	no	yes	yes	yes	IMDA PDPC
P.R.China	N/A	N/A	N/A	N/A	N/A	
Cook Islands	Opt-in	yes	yes	yes	no	Office of the PM

Lao PDR	Lao PDR does not have specific regulation on unsolicited SMS/MMS.					
Malaysia	Malaysia does not have specific regulation on unsolicited SMS/MMS.					
New Zealand	Opt-in	yes	yes	yes	no	DIA
Hong Kong	Opt-out	no	yes	yes	yes	OFCA
India	India does not have specific regulation on unsolicited SMS/MMS.					
Indonesia	Opt-out	no	N/A	yes	N/A	MCI
Thailand	N/A	N/A	N/A	N/A	N/A	
Pakistan	Opt-in	yes	no	yes	no	PTA
Papua New Guinea	N/A	N/A	no	no	no	NICTA
Philippines	Opt-in	yes	yes	yes	no	NTC
Viet Nam	Opt-in	yes	yes	yes	yes	MIC
Bhutan	Bhutan does not have specific regulation on unsolicited SMS/MMS.					
Brunei	Brunei does not have specific regulation on unsolicited SMS/MMS.					
Cambodia	Cambodia does not have specific regulation on unsolicited SMS/MMS.					
Micronesia (Federated States of)	Micronesia does not have specific regulation on unsolicited SMS/MMS.					
Nepal	Nepal does not have specific regulation on unsolicited SMS/MMS.					
Kiribati	Kiribati does not have specific regulation on unsolicited SMS/MMS.					
Sri Lanka	Sri Lanka does not have specific regulation on unsolicited SMS/MMS.					
Tonga	Tonga does not have specific regulation on unsolicited SMS/MMS.					

*In Singapore, only bulk emails and messages are regulated.

Regulations on spam e-mail and spam SMS/MMS (hereafter spam messages) are regulated by the same laws in most countries and have the same tendency. However, in some countries, different laws apply to spam e-mails and spam messages, so there are differences in regulatory framework.

Regarding the regulation on spam messages, 9 of the 25 countries studied (Australia, Cook Islands, Republic of Korea, Japan, Singapore, New Zealand, Hong Kong, Philippines, and Viet Nam) have a comprehensive system of legislation on spam messages. These countries have adopted an opt-in (Australia, Cook Islands, Republic of Korea, Japan, New Zealand, Philippines, Viet Nam) or opt-out (Singapore, Hong Kong) method to control spam, regardless of the method, a systematic regulatory framework to protect users from spam is equipped with

these countries. Australia, Cook Islands, Japan, Singapore, New Zealand, and Hong Kong have enacted separate spam message laws. Republic of Korea, although not an individual spam message law, has a separate section on spam in the Information and Communication Network Act to regulate spam messages specifically and systematically. Philippines has enacted separate administrative regulations to regulate spam messages, and Viet Nam has enacted enforcement decree to comprehensively regulate spam messages.

Indonesia did not have direct regulations on spam messages, but in 2021 Indonesia enacted a decree to regulate spam SMS. So, even though the decree cannot be considered as a comprehensive law, now Indonesia is regulating SMS directly. Pakistan has an opt-in system by stipulating that the Electronic Crimes Act prohibits sending SMS without permission and without an unsubscribe facility. PNG regulates spam based on Cybercrime Code Act.

Cambodia, Lao PDR, Malaysia, Nepal, India, Bhutan, Brunei, Micronesia (Federated States of), Kiribati, Tonga and Sri Lanka do not have direct and specific law or enforcement decree or administrative regulations on spam messages. However, these countries are also divided into Cambodia, Sri Lanka, Brunei, Micronesia (Federated States of), Lao PDR, Tonga, and Bhutan, which do not regulate spam messages, and Malaysia, Nepal, India, and Kiribati, which regulate spam messages to a certain level.

Malaysia does not have direct regulations against spam messages, but 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 a violation of the law. Of course, as discussed above, this regulation has limitations, but Malaysia is trying to regulate some of the spam messages.

In the case of Kiribati, there are no direct regulations on spam messages. However, the Cybercrime Act 2021 covers in principle the nature of spam relating to unauthorized computer system access or unauthorized computer system interference should the spam carry a malicious payload to a computer system, interfering with its normal operation.

P.R.China did not provide information on spam message regulation in the survey this year, and there was a lack of relevant publicly available information.

The similarities and differences between countries that have a comprehensive regulatory system for spam messages are as follows.

1) Similarities

Whether the statute adopted an opt-in method or an opt-out method, the core regulations were found to be similar.

(1) Provide accurate sender information

Countries with comprehensive spam control systems, whether adopting the opt-in method or the opt-out method, have in common that the sender provides accurate sender information to the recipient. Of course, there are some differences in the type of information provided, but it is basically required to provide accurate reply e-mail address, and in some cases to provide the name, address, and phone number of other senders.

Country	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)

(2) Provide unsubscribe facility

Countries with comprehensive spam control systems, whether adopting the opt-in method or the opt-out method, have in common that the sender provides the receiver with an unsubscribe

facility. There are many cases where the unsubscribe facility is basically an electronic address or phone number, but there are cases where specific means are not specified.

Country	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

2) Differences

(1) Prior consent of recipient

In the case of countries adopting the opt-in system (Australia, Korea, Japan, Philippines, New Zealand, Vietnam), it is stipulated that prior consent must be obtained due to the nature of opt-in. In the case of opt-out (Singapore, Hong Kong), a message can be sent without prior consent. However, if the recipient notifies of their intention to reject the message after receiving the message, the sending of additional messages is stopped.

Country	Prior consent
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
Singapore	no
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
Hong Kong	no
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.

(2) Labeling obligation

Many countries with comprehensive anti-spam legislation have labeling obligations. In the case

of labeling, it is easier for users to check whether the message is an advertisement message or not, and it is an effective regulatory measure because the burden on the sender due to labeling is not so large. However, whether the labeling obligation is applied or not, the necessity should be reviewed in consideration of the various situation and circumstances of the country concerned.

Country	**Labeling obligation**
Australia	No
Cook Islands	No
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.
Philippines	No
New Zealand	No
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.

(3) Bulk requirement

Unlike other countries, Singapore is subject to regulate spam message only if it meets the bulk requirement. For other countries, there are no such bulk requirement.

Country	Bulk requirement
Australia	No
Cook Islands	No
Republic of Korea	No
Japan	No
Singapore	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;
Philippines	No
New	No

Zealand	
Hong Kong	No
Viet Nam	No

3.2.2. Policy implications from spam legislation

As mentioned above, the anti-spam laws of major member countries are diverse, such as adopting opt-in or opt-out. As the opt-in and opt-out methods each have their own strengths and weaknesses, Members have established their spam regulation system by reflecting their own circumstances. However, as seen above, for effective spam regulation, it is necessary to provide accurate sender information to the recipients regardless of opt-in/opt-out, and to include unsubscribe facility for opting out. In addition, if possible, it seems necessary to require the sender to indicate that the sent e-mail/message is an advertisement in the subject line, and to regulate the use of address harvesting software or the use of address lists automatically collected through it.

However, if you put together the contents reviewed above, in the end, the spam control law should be flexibly developed to suit each country's situation and environment. Each country will be able to come up with legislation by referring to the various examples above. APT has plans to support legislation in the field of spam control through expert missions and training courses, so Members in need may request such assistance.

3.2.3. Comparative analysis on spam policy

Member	Technical measures	Self-regulation	Education/ campaign	International cooperation	Other issues
Australia	Spam filtering by telecommunication/ internet service providers	No / The direct regulatory model remains appropriate.	ACMA provides education to both industry and consumers	UCENet/ MoUs with both the USA and Canada/ RCEP agreement	
Cambodia	MaxBIT spam filter	No	No	No	
Cook Islands	N/A	No	N/A	No	
Republic of Korea	KCC and KISA develop and	Spam distribution	For business operators; business	GSMA global project/	

Member	Technical measures	Self-regulation	Education/ campaign	International cooperation	Other issues
	distribute software to block spam. KISA-RBL, KISA-MRBL, White domain, SPF	status report (half yearly)	briefing sessions and educational content production/ For users; production of educational materials and educational contents	UCENet/ UCENet Asia-Pacific(Korea, Australia,Japan, New Zealand, Taiwan) / RCEP agreement	
Japan	N/A	N/A	N/A	UCENet/ RCEP agreement	
Singapore	blocking scam SMS/calls	Spam control guidelines/ Code of practice by industry association	Public education	RCEP agreement, MoU with ACMA Australia	
P.R.China	N/A	N/A	Education/awareness raising	UCENet/ RCEP agreement	
Lao PDR	SMS inspection system	No	No	RCEP agreement	
Malaysia	N/A	N/A	Education/awareness raising	UCENet/ RCEP agreement	
Nepal	No	No	No	No	
New Zealand	N/A	Code of practice by private associations	N/A	RCEP agreement	
Hong Kong	Do-not-call register (fax, SMS, pre-recorded telephone message)	Code of practice by private associations	education and publicity programmes to educate the public; public seminars, roving exhibitions	Free Trade Agreement between Hong Kong, China and Australia/ UCENEt	AI/chatbot
India	N/A	N/A	N/A	N/A	
Indonesia	No	No	Education and	RCEP	

Member	Technical measures	Self-regulation	Education/ campaign	International cooperation	Other issues
			awareness raising policy	agreement	
Thailand	Mail cleaner service by internet service provider	Code of Practice	no	RCEP agreement	
Pakistan	Anti-spam filters	No	Public awareness messages, Advertisement	No	
Papua New Guinea	No	No	Awareness raising through media	No	
Philippines	N/A	N/A	N/A	RCEP agreement	
Viet Nam	Spam portal	N/A	N/A	RCEP agreement	
Bhutan	N/A	No	No	No	
Brunei	Technical measures by network operator	No	general online safety awareness program; online safety learning materials, publish videos, audios and awareness materials for broadcast, awareness talks	RCEP agreement	
Micronesia (Federated States of)	Technical measures by Telecon Corporation	No	No	No	
Kiribati	N/A	No	No	No	
Sri Lanka	Technical measures by each organization	No	Education and awareness through social media, sending SMS to subscribers by operators	No	
Tonga	No	No	No	No	

A. Technical response

As mentioned above, in many countries, technical filtering measures by private Internet service providers were the most important technical measures related to spam response. Australia, Cambodia, Republic of Korea, Thailand, Brunei, Micronesia (Federated States of), Lao PDR, Pakistan, Singapore, and Sri Lanka explicitly mentioned technical measures by telecommunication service providers. However, it is presumed that similar technical measures such as filtering by service providers are taking place in countries that have not explicitly provided relevant information. Regarding technical response, it was surveyed that Republic of Korea is taking government-led technological measures. In Korea, the Information and Communications Network Act stipulates that the government can develop and distribute software to block spam. Accordingly, KCC and KISA actually prepared KISA-RBL (Realtime Blocking List), KISA-MRBL (Mobile Realtime Blocking List), White domain (a kind of whitelist), and SPF (Sender Policy Framework) and provide them to service providers.

B. Self-regulation

Regarding self-regulation, it was confirmed that Republic of Korea, New Zealand, Hong Kong, Thailand, and Singapore have self-regulation systems. Republic of Korea issues a spam distribution status report (half yearly) and regularly announces the amount of spam distribution by service providers, thereby enhancing the voluntary spam reduction efforts of telecommunication service providers. To this end, indexes that can be compared with each service provider's efforts to reduce the amount of spam distribution are prepared and operated.

Singapore, New Zealand, Thailand, and Hong Kong promote voluntary spam reduction efforts of service providers by creating and using private business associations' code of practice. Singapore has also developed spam control guidelines with ISPs.

In the case of Australia, as discussed above, a study was conducted on the introduction of self-regulation at the government level. According to this study, government direct regulation is more appropriate than self-regulation considering domestic conditions such as the level of cooperation between service providers in Australia and overseas cases. It seems that most Members, as well as Australia, rely more on direct regulation than on self-regulatory systems.

C. Education and Awareness raising

It was confirmed that Australia, Republic of Korea, P.R.China, Indonesia, Pakistan, PNG, Singapore, Malaysia, Hong Kong, Brunei, and Sri Lanka are conducting business/user education and awareness-raising activities at the government level. In addition, it is estimated that several other countries are engaged in such activities, but there was insufficient information to confirm the rest.

In Australia, ACMA provides training to industry stakeholders and users. Republic of Korea conducts business briefing sessions and educational content production for business operators

and produces educational materials and educational contents for users. P.R.China and Malaysia are engaged in education/awareness raising activities, and Hong Kong is operating education and publicity programs such as public seminars and roving exhibitions. The Brunei government provides online safety learning materials, awareness talks, and also publishes videos, audios and awareness materials for broadcast, etc. in its online safety awareness program. Sri Lanka conducts education and awareness raising through social media and sends SMS to subscribers by service providers.

D. International cooperation

Since spam inherently affects across borders, Members seem to generally agree on the need for international cooperation to combat spam. Nevertheless, just some countries are actively participating in international cooperation initiatives. Among the international cooperation initiatives in which Members are participating, a representative example is the UCENet discussed above. Australia, Republic of Korea, Japan, P.R.China, Malaysia and Hong Kong have been participating in this initiative, which started as the London Action Plan and continued more than 15 years. In particular, Republic of Korea has sought to strengthen cooperation within the region by establishing UCENet Asia-Pacific, which is a regional initiative of UCENet.

Recently, a number of Members (Australia, Republic of Korea, Japan, Singapore, P.R.China, Lao PDR, Malaysia, New Zealand, Indonesia, Thailand, Philippines, Viet Nam, Brunei, etc.) have signed the RCEP Agreement. Through this, cooperation on spam response activities in the region can be strengthened, and each country's efforts to counter spam can also be promoted. It is expected that this agreement will serve as an opportunity to advance cooperation in response to spam in the Asia-Pacific region.

3.2.4. Policy implications from spam policies

As mentioned above, the policy measures to prevent spam in Members also show various aspects in each country. In terms of technical measures, self-regulation, education and awareness-raising activities, and international cooperation activities, Members have established their spam policies by reflecting their own circumstances. However, as shown above, for effective spam control, it is necessary to prepare technical measures at the government level in addition to business-centered filtering, strengthen self-regulation, education, and awareness-raising activities, and seek to establish an international cooperative system and strengthen cooperative activities. However, it is noteworthy that many countries have recently shown a tendency to strengthen direct regulation of regulatory authorities rather than non-regulatory self-regulation.

However, if you put together the contents reviewed above, in the end, the spam control policy should be flexibly developed to suit each country's situation. Each country will be able to come up with policies by referring to the various examples above. APT has plans to support policy development in the field of spam control through expert missions and training courses, so Members in need may request such assistance.

4. Way Forward

Spam control has been a long-standing challenge, but it is an area that is constantly evolving, and regulators must adapt to keep up. The reality is that unsolicited communications are becoming increasingly complex and difficult to regulate. This phenomenon is exacerbated by technologies that make it possible to send unsolicited communications in bulk, fast and inexpensively. Emerging technologies, including the proliferation of VoIP, robocalls, and spam via social media, make spam control even more difficult. The rapid pace of technological change that challenges the legislative and regulatory capacity of regulator is one of the biggest challenges for each country today.

The increasing internationalization of unsolicited communications increases the difficulty of cross-border investigations and enforcement, and the lack of resources and manpower of regulatory agencies related to cracking down on unsolicited communications is a chronic issue and makes it difficult to solve the problem.

Even though worldwide efforts to combat spam has been strengthened due to this situation, in Asia-Pacific region, we don’t have relevant and updated information on the current status of spam response from APT Members.

So, 2021-2023 APT-KISA 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.

Since this research will be conducted for three years and 2022 is the second year of this research project.
In 2021 and 2022, research team conducted the survey on APT Members (including Associate Members)’ anti-spam policy, issues, and legislation to figure out the current status of members regarding spam control.

As found above, when review the results of these two years’ survey, many APT Members still do not have comprehensive legal systems for spam control. For spam email, only 9 of the 25

countries studied during last two years have comprehensive anti-spam legislation. In addition, policy efforts to prevent spam are often somewhat insufficient, and only some countries have an international cooperation scheme to cooperate with other countries and international organizations.

It would be best if all Members could enact comprehensive spam control act, provide systematic and continuous policy support, and strengthen international cooperation efforts by establishing international cooperation system or participating in existing initiatives. However, due to economic, legal, and cultural diversity, some APT Members may find it difficult to enact comprehensive spam control laws, provide continuous policy support, or participate in international spam control initiatives.

Nevertheless, there is room for improvement for APT Members in the field of spam control. Although it is difficult to enact a comprehensive spam control law, efforts are needed to add new provisions that meet global standards or to revise some of the existing laws while maintaining the current legal system. By referring to the legal examples of leading countries in the Americas, Europe and Asia-Pacific region presented in this study, Member States can make choices such as which new legal provisions to be added to existing laws or which parts of existing laws to be amended. The goals can be: 1) Providing accurate sender information, 2) Providing unsubscribe facility, 3) Prior consent, 4) Providing of labeling, 5) Prohibition of use of address harvesting software and automatically harvested address list.

The same is true in the field of spam control policies. 1) Providing technical support at the government level, 2) introducing self-regulation, 3) strengthening education and awareness-raising activities, 4) strengthening international cooperation, etc. can be sought. In particular, if it is difficult to establish a new bilateral or multilateral cooperation system for spam control in relation to international cooperation, each country can participate in existing international cooperation initiatives such as UCENet. This can improve the level of spam control in society as a whole and increase trust in the Internet.

The ultimate goal of this research project is to find common elements and consider possible measures to mitigate impact of unsolicited commercial messages (spam) in the Asia-Pacific region. So, to this end, in 2023 research team plans to conduct (1) additional fact-finding surveys on the remaining Members that did not submit survey results during last two years, (2) analysis of problems/limitations of current international cooperation measures based on the results of the survey and desk study, (3) research to find common elements and consider possible measures to mitigate the impact of spam in the Asia-Pacific region.

From this point of view, this research plans to provide more detailed information on spam legislation, policies, and international cooperation systems in the future. Members can refer to this information to legislate or amend some existing laws related to spam, or to introduce

policies and international cooperation measures that are appropriate to the situation/environment of each country. Members will be able to find the best option for their situation from among the various alternatives reviewed in this research.

In particular, APT plans to help Members through various work programmes such as Expert Mission and Training courses. The APT Secretariat will develop training courses in collaboration with KISA to provide information on global norm, trends, legislation, and policy in the field of spam, which will be available to APT Members upon request basis. In addition, as part of the APT Expert Mission, APT Secretariat also provide consulting on spam control legislation, policies, and international cooperation measures when there is a request from Members. APT will continue to work with Members to ensure that these efforts continue.

References

[1] APT, “The Strategic Plan of the Asia-Pacific Telecommunity for 2021-2023”, https://www.apt.int/sites/default/files/Upload-files/GA-MC-DOCS/2020-GA15-MC44/Strategic_Plan_2021-2023.pdf

[2] KCC, Korea, “Comprehensive Measures for Spam Prevention”, 21. January, 2011

[3] ACMA, “Unsolicited Communications Research; A Study of International Best Practice”, https://www.acma.gov.au/sites/default/files/2019-08/ACMA-UC-Research-Findings-Report-May-2018.pdf

[4] EU, “Convention on Cybercrime 2001”, https://rm.coe.int/1680081561

[5] EU, “EU e-privacy directive”, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML

[6] ACCC, “London Action Plan”, https://www.accc.gov.au/system/files/The%20London%20action%20plan%20on%20international%20spam%20enforcement%20cooperation.pdf

[7] OECD, “Report of the OECD Task Force on Spam: Anti-spam toolkit of Recommended Policies and Measures”, https://www.oecd.org/sti/consumer/36494147.pdf

[8] UCENet webpage, “Who We Are, History, Member organizations”, https://www.ucenet.org/who-we-are/

[9] ITU, “Unsolicited Commercial Communications-an overview of challenges and strategies”, https://www.itu.int/dms_pub/itu-d/oth/07/27/D07270000010001PDFE.pdf

[10] ITU, “Question 6/1: Consumer information, protection and rights: Laws, regulation, economic bases, consumer networks”, https://www.itu.int/pub/D-STG-SG01.06.3-2017

[11] ITU, “Unsolicited Commercial Communications/ Nuisance calls: Are consumers more vulnerable in the era of COVID-19?”, https://www.itu.int/en/ITU-D/Study-Groups/2018-2021/Pages/meetings/Webinars/2020/Q6-1-july02.aspx

[12] ITU, “ITU-D Study Groups - Ongoing Work”, https://www.itu.int/en/ITU-D/Study-Groups/2018-2021/Pages/OngoingWork.aspx

[13] ITU, “Anti-Spam Laws and Authorities Worldwide”, https://www.itu.int/osg/spu/spam/law.html

[14] OECD, “Task force on Spam”,

https://web.archive.org/web/20080827191919/http://www.oecd-antispam.org/countrylaws.php3

[15] IAPP, “The case of the unsolicited email”, https://iapp.org/news/a/the-case-of-the-unsolicited-email/

[16] Federal Register, “Controlling the Assault of Non-Solicited Pornography and Marketing Rule”, https://www.federalregister.gov/documents/2019/04/04/2019-06562/controlling-the-assault-of-non-solicited-pornography-and-marketing-rule

[17] ESPC, “Fighting Spam, Educating Members on Best Practices, Law, and industry Developments to Fight Spam and Protect Email and a Viable and Essential Communications Tool”, https://www.espcoalition.org/overview

[18] Spam laws website, “Anti-spam Laws”, https://www.spamlaws.com/world.shtml

[19] Light span digital, “What You Need to Know About Anti-Spam Laws Around the World”, https://lightspandigital.com/blog/need-know-anti-spam-laws-around-world/

[20] WTO, WTO e-commerce negotiations, https://www.wto.org/english/news_e/news21_e/ecom_05feb21_e.htm

[21] KOSEN, “Main contents and implications of trade rules in RCEP agreement related to cross-border data transfer”, https://www.kosen21.org/info/gtbReport/gtbReportDetail.do?articleSeq=GTB_000000000015514 1

[22] Chamaileon, “The Ultimate Email SPAM Law Collection – 28 Countries Included”, https://chamaileon.io/resources/ultimate-email-spam-law-collection/

[23] Center for Internet & Society, “Anti-Spam Laws in Different Jurisdictions: A Comparative Analysis”, https://cis-india.org/internet-governance/blog/anti-spam-laws-in-different-jurisdictions

[24] ACMA, “Action on spam and telemarketing”, https://www.acma.gov.au/action-spam-and-telemarketing

[25] Federal Register, “Spam Act 2003”, Spam Act 2003 (legislation.gov.au)

[26] Federal Register, “Do Not Call Register Act 2006”, https://www.legislation.gov.au/Details/C2021C00356

[27] Media buzz, “Asian Anti-Spam Guide”, https://mediabuzz.com.sg/mediabuzz_supplements/asg.pdf

[28] ITU, “Asia Pacific Legislative Analysis”, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf

[29] ACMA, “Report on industry self-regulation of commercial electronic messages, the Do

Not Call Register and the Integrated Public Number Database”, https://www.acma.gov.au/sites/default/files/2019-10/Report-to-the-Minister-for-Communications-on-self-regulation-of-functions_0.pdf

[30] ACMA, “Memorandum of Understanding”, https://www.acma.gov.au/memorandums-understanding

[31] KCC, Spam distribution status report 2020 second half, https://kcc.go.kr/user.do?mode=view&page=A05030000&dc=K00000200&boardId=1113&boardSeq=50925

[32] Korean Law Information Center, “Act on Promotion of Information and Communications Utilization and Information Protection”, https://www.law.go.kr/engLsSc.do?menuId=1&subMenuId=21&tabMenuId=117&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D#

[33] Japan Data Communications Association, “Overview of Japanese Anti-Spam Law”, https://www.dekyo.or.jp/soudan/contents/antispam/data/en/EN_Overview_of_Japanese_Anti-Spam_Law.pdf

[34] World Laws Information Center, “The Act on Regulation of the Transmission of Specified Electronic Mail”, https://world.moleg.go.kr/web/wli/lgslInfoListPage.do?A=A&searchType=all&searchText=%25EC%25A0%2584%25EC%259E%2590%25EB%25A9%2594%25EC%259D%25BC&searchPageRowCnt=10&searchNtnlCls=1&searchNtnl=JP&pageIndex=1

[35] MIC, Japan, “The Act on Regulation of the Transmission of Specified Electronic Mail”, https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_4.pdf

[36] IMDA website, “Unsolicited Communications”, https://www.imda.gov.sg/for-community/Infocomm-regulation-and-guides/unsolicited-communications

[37] Singapore Statutes Online, “Spam Control Act”, https://sso.agc.gov.sg/Act/SCA2007

[38] Singapore Spam Control Resource Center website, https://web.archive.org/web/20080915211550/http://www.spamcontrol.org.sg/

[39] IMDA website, “Singapore Law to Control Spam”, https://www.imda.gov.sg/news-and-events/Media-Room/archived/ida/Media-Releases/2007/20060919202026

[40] Singapore Statutes Online, “Personal Data Protection Act”, https://sso.agc.gov.sg/Act/PDPA2012

[41] ISOC China, “China to regulate Internet Email Services”, https://www.isc.org.cn/english/Specails/Anti-Spam_Initiatives/listinfo-15413.html

[42] Lehman, Lee & Xu, “Measures for the Administration of Internet E-mail Services 2006”, http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-

technology/measures-for-the-administration-of-internet-e-mail-services-2006.html

[43] Sampi, “China Email Marketing and Chinese Anti-Spam Laws”, https://sampi.co/email-marketing-and-chinas-anti-spam-laws/

[44] Benchmark Internet Group, “Maintaining Compliance with China’s Severe Email Marketing”, https://www.benchmarkemail.com/blog/maintaining-compliance-with-chinas-severe-email-marketing-laws/

[45] Haiping Zheng, “Regulating the Internet: China’s Law and Practice”, 4. January, 2013

[46] MCMC website, “Spam Laws”, https://www.mcmc.gov.my/en/faqs/spam/spam-laws/spam-laws

[47] MCMC website, “Legislation”, https://www.skmm.gov.my/en/legal/acts

[48] DIA, New Zealand, “Spam Prevention & Messaging Compliance”, https://www.dia.govt.nz/Spam

[49] Parliamentary Counsel Office, New Zealand, “Unsolicited Electronic Messages Act 2007”, https://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html

[50] OFCA, “Enforcement Statistics of Unsolicited Electronic Messages Ordinance (UEMO)”, https://www.ofca.gov.hk/filemanager/ofca/en/content_296/eng_enf_uemo.pdf

[51] OFCA, “Unsolicited Electronic Messages Ordinance”, https://www.ofca.gov.hk/en/consumer_focus/guide/others/uemo/index.html

[52] Hong Kong e-Legislation, “Unsolicited Electronic Messages Ordinance”, https://www.elegislation.gov.hk/hk/cap593

[53] OFCA, Do-Not-Call Register website, https://www.dnc.gov.hk/public/#/en/home

[54] Kominfo, Indonesia, “Indonesia Law on Information and Electronic Transactions”, https://aptika.kominfo.go.id/2019/08/undang-undang-ite/

[55] Flevin, “Indonesia Law on Information and Electronic Transactions”, http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4846_UU_11_2008_e.html

[56] Kominfo, Indonesia, “Indonesia Law on Information and Electronic Transactions”, https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april++2008

[57] MDES, Thailand, “Computer-Related Crime Act 2007”, https://www.mdes.go.th/law/detail/3618-COMPUTER-RELATED-CRIME-ACT-B-E--2550--2007-

[58] NTC, Philippines, “Rules and regulations on Broadcast messaging service (2005)”,

https://ntc.gov.ph/wp-content/uploads/2015/10/LawsRulesRegulations/MemoCirculars/MC2005/MC-03-03-2005.pdf

[59] NTC, Philippines, "Amendment to the Rules and regulations on Broadcast messaging service (2006)", https://ncr.ntc.gov.ph/wp-content/uploads/2019/Memorandum_Circulars/2006/MC-03-03-2005A.pdf

[60] NTC, Philippines, "Further amending memorandum circular (Rules and regulations on Broadcast messaging service) (2009)", https://ntc.gov.ph/wp-content/uploads/2015/10/LawsRulesRegulations/MemoCirculars/MC2009/MC-04-07-2009.pdf

[61] NTC, Philippines, "Further amending memorandum circular (Rules and regulations on Broadcast messaging service) (2018)", https://ntc.gov.ph/wp-content/uploads/2018/MC/MC-07-08-2018.pdf

[62] BOI, Philippines, "Public Telecommunications Policy Act", https://boi.gov.ph/wp-content/uploads/2018/02/RA-7925.pdf

[63] Official Gazette, "Cybercrime Prevention Act", https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

[64] WIPO, Viet Nam, "Law on Information Technology", https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/vn/vn134en.html

[65] Vanbanphapluat, "Decree 91 on fighting spam messages, spam emails and spam calls",

https://vanbanphapluat.co/decree-91-2020-nd-cp-fighting-spam-messages-spam-emails-and-spam-calls

[66] Tilleke & Gibbins, "Vietnam's New Decree 91 Sets Out Stricter Anti-Spam Regulations", https://www.tilleke.com/insights/vietnams-new-decree-91-sets-out-stricter-anti-spam-regulations/

[67] LuatVietnam, "Decree No. 91/2020/ND-CP fighting spam messages, spam emails and spam calls", https://english.luatvietnam.vn/decree-no-91-2020-nd-cp-dated-august-14-2020-of-the-government-on-fighting-against-spam-text-messages-spam-emails-and-spam-calls-189003-Doc1.html

[68] Legal Services India, "Email Privacy & Anti-spam Law", http://www.legalservicesindia.com/article/107/Email-Privacy-&-Anti-spam-Law.html#:~:text=That%20law%20is%20called%2C%20The,electronic%20mail%20through%20the%20internet.

[69] NCR News, "Is Spam illegal? Know more About Anti-Spam Laws in India", https://www.ncr.news/legal/is-spam-illegal-know-more-about/[70] Indian Review of

Advanced Legal Research, “The Chronic Plight of Spamming In India”, https://www.iralr.in/post/the-chronic-plight-of-spamming-in-india

[71] Prabodh Shukla, “Spamming in India”, https://www.studocu.com/en-nz/document/university-of-waikato/legal-aspects-of-cyber-security/spamming-in-india/17789284

[72] Chambers and Partners, “Data Protection and Privacy 2022”, https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2022/india

[73] Boloji, “A Comparison of Spam Laws between India & The U.S.”, https://www.boloji.com/articles/52001/a-comparison-of-spam-laws

[74] CamCERT, “How to Reduce Spam”, https://www.camcert.gov.kh/%e1%9e%9c%e1%9e%b7%e1%9e%92%e1%9e%b8%e1%9e%9f%e1%9e%b6%e1%9e%9f%e1%9f%92%e1%9e%8f%e1%9f%92%e1%9e%9a%e1%9e%80%e1%9e%b6%e1%9e%8f%e1%9f%8b%e1%9e%94%e1%9e%93%e1%9f%92%e1%9e%90%e1%9e%99-spam/

[75] Maxbit, “Anti-Spam Filtering Service”, https://maxbit.com.kh/cn/we-build-responsive-website-template-for-all-your-needs/

Annex 1. APT Letters

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

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!

Annex 3. The Act on Regulation of the Transmission of Specified Electronic Mail (Japan, translated in English) (Act No. 26 of April 17, 2002)

Chapter I General Provisions

Article 1 (Purpose)

The purpose of this Act, in light of the recognized need to prevent the occurrence of disturbances upon the transmission and reception of Electronic Mails due to simultaneous transmission, etc. of Specified Electronic Mails to many persons, is, by specifying measures, etc. for proper transmission of Specified Electronic Mails, to create a preferable environment for the use of Electronic Mails, and thereby to contribute to the sound development of an advanced information and communications society.

Article 2 (Definitions)

In this Act, for the meanings of the terms given in the following items, the definition specified in each item shall apply.

(i) The term “Electronic Mail” means telecommunications (referring to telecommunications as specified under Article 2 item (i) of the Telecommunications Business Act (Act No. 86 of 1984)) to transmit information, including texts, to specified persons by having the screens of communications terminals (including input/output devices; the same shall apply hereinafter) used by said specified persons display said information, and which uses communications methods specified in the applicable Ministry of Internal Affairs and Communications (hereinafter, "MIC") ordinance.

(ii) The term “Specified Electronic Mail” means Electronic Mail, which a person who sends Electronic Mail (limited to transmissions from telecommunications facilities (referring to telecommunications as specified under Article 2 item (ii) of the Telecommunications Business Act; the same shall apply hereinafter) in Japan or transmission to telecommunications facilities in Japan; the same shall apply hereinafter) (limited to an organization for profit and a person in cases where the person is engaged in business; hereinafter, "sender") sends as a means of advertisement or propaganda for their own sales activities or for others.

(iii) The term “Electronic Mail Address” means codes, including characters, numerical characters, and marks, for identifying a user of Electronic Mail.

(iv) The term “Fictitious Electronic Mail Address” means an Electronic Mail Address falling under both of the following conditions:

(a) An Electronic Mail Address as produced by using a program (referring to a set of orders to a computer, and orders of which are combined for obtaining a result) with a function to automatically generate many Electronic Mail Addresses

(b) An Electronic Mail Address actually not being used by anyone as an Electronic Mail Address

(v) The term “Electronic Mail Services” means telecommunications services pertaining to Electronic Mail as provided for in Article 2 item (iii) of the Telecommunications Business Act.

Chapter II Measures for the Appropriate Transmission of Specified Electronic Mail

Article 3 (Limitation of Transmission of Specified Electronic Mail)

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

(ii) In addition to those listed in the preceding item, a person who has notified, as specified in the applicable MIC ordinance, the sender, or the consignor of transmission of his/her own Electronic Mail Address

(iii) In addition to those listed in the preceding two items, a person who has a business relationship with a person engaged in sales activities relating to advertisement or propaganda that employs the said Specified Electronic Mail as its means

(iv) In addition to those listed in the preceding three items, an organization or a person who has made, as specified in the applicable MIC ordinance, his/her address public (limited to those who engage in business in the case of a person)

(2) A person who has received the notification set forth in item (i) of the preceding paragraph shall maintain, as specified in the applicable MIC ordinance, a record that proves the fact that a request was made to send Specified Electronic Mail or that consent was made to send Specified Electronic Mail.

(3) When a sender has received notice of a request not to send Specified Electronic Mail (or, in cases where the request was not to send Specified Electronic Mail pertaining to certain matters, the said request) (including cases where a consignor of transmission has received such notification) from any person specified in the items of paragraph (1) in accordance with the applicable MIC ordinance, the sender shall not send Specified Electronic Mail against the notifying party's intention indicated in the said notice, provided, however, that this shall not apply to cases where advertisement or propaganda is made appendant in an Electronic Mail that is sent based on the intention of the person who receives the Electronic Mail sent mainly for purposes other than advertisement or propaganda and other similar cases as specified in the applicable MIC ordinance.

Article 4 (Obligation of Labeling)

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 (except the matters listed in item (ii) for those cases specified in the applicable MIC ordinance under the proviso of paragraph (3) of the preceding article) 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 under the main clause of paragraph (3) of the preceding article, 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

Article 5 (Prohibition of Transmission under False Sender Information)

No sender shall send Specified Electronic Mails falsifying the following information on the sender among information for sending and/or receiving Electronic Mails (hereinafter, "sender information"):

(i) Electronic Mail Address used for sending the said Electronic Mails

(ii) Codes, including characters, numerical characters, and marks, for identifying telecommunications facilities for sending the said Electronic Mails

Article 6 (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.

Article 7 (Administrative Order)

Where the Minister for Internal Affairs and Communications (hereinafter, the Minister) deems that with respect to the transmission of Electronic Mails, including simultaneous transmission of Specified Electronic Mails to many persons, a sender does not comply with the provisions of Article 3 or Article 4, or where the Minister deems that a sender has sent Electronic Mails using false sender information or Electronic Mails to Fictitious Electronic Mail Addresses, and when the Minister deems that it is necessary to prevent the occurrence of disturbances upon transmission and reception of Electronic Mails, the Minister may order the said sender (or, in cases where the consignor of transmission related to these Electronic Mails has conducted part of the services related to the transmission of the said Electronic Mails, including receiving the notification under item (i) or item (ii) of Article 3 paragraph (1) regarding the transmission of the said Electronic Mails, maintaining the record under paragraph (2) of the same article and

others, and when it is deemed that there is a cause attributable to the said consignor related to the transmission of the said Electronic Mails, the said sender and the said consignor of transmission) to take necessary measures to improve the methods for Electronic Mail transmission.

Article 8 (Petition to the Minister)

A person who has received Specified Electronic Mail may, when it is deemed that Specified Electronic Mail has been sent in violation of the provisions of Article 3 through Article 5, petition the Minister to take proper measures.

(2) A person who is offering an Electronic Mail Service may, when it is deemed that Electronic Mail has been sent to Fictitious Electronic Mail Addresses in violation of the provisions of Article 6, petition the Minister to take proper measures.

(3) The Minister shall, when receiving a petition pursuant to the provisions of the preceding two paragraphs, implement the necessary investigation, and where it is deemed necessary based upon the results of the investigation, take measures based upon this Act and other proper measures.

Article 9 (Dealing with Complaints, etc.)

Any sender of Specified Electronic Mails shall, in good faith, deal with complaints, inquiries, etc. on transmission of the Specified Electronic Mails by the sender.

Article 10 (Information Provision and Technological Development, etc. by Telecommunications Carriers)

Any telecommunications carrier (referring to a telecommunications carrier stipulated in Article 2 item (v) of the Telecommunications Business Act; hereinafter the same shall apply) offering Electronic Mail Services shall endeavor to provide users of said services with information on services that contribute to preventing the occurrence of disturbances upon transmission and reception of Electronic Mails caused by Specified Electronic Mails, Electronic Mails using false sender information or Electronic Mails being sent to Fictitious Electronic Mail Addresses (hereinafter, "Specified Electronic Mail, etc.").

(2) Any telecommunications carrier offering Electronic Mail Services shall endeavor to develop or introduce technologies that contribute to preventing the occurrence of disturbances upon transmission and reception caused by Specified Electronic Mail, etc.

Article 11 (Refusal to Provide Telecommunications Services)

A telecommunications carrier may, in cases where an Electronic Mail using false sender information has been sent and when it is deemed that there is a risk of causing disturbances in offering smooth Electronic Mail Services, or causing disturbances upon transmission and reception of Electronic Mails to users of the services, where many Electronic Mails being sent to Fictitious Electronic Mail Addresses have been simultaneously sent and when it is deemed

that there is a risk of causing disturbances in offering smooth Electronic Mail Services, or where it is deemed that there is justifiable grounds to refuse the provision of Electronic Mail Services to prevent the occurrence of disturbances upon transmission and reception of Electronic Mails, refuse to provide Electronic Mail Services to a person who sends Electronic Mails that have a risk of causing said disturbances, to the extent necessary to prevent said disturbances.

Article 12 (Instruction and Advice to Corporations for Telecommunications Carriers)

The Minister shall endeavor to give the necessary instructions and advice for services to a juridical person incorporated pursuant to the provisions of Article 34 of the Civil Code (Act No. 89 of 1896), which provides member telecommunications carriers with services, including the provision of information, contributing to preventing the occurrence of disturbances upon transmission and reception of Electronic Mails caused by Specified Electronic Mails, etc.

Article 13 (Disclosure of Status of Research and Development, etc.)

The Minister shall, at least once a year, disclose the status of research and development on technologies for contributing to preventing the occurrence of disturbances upon transmission and reception of Electronic Mails caused by Specified Electronic Mails, etc. and the status of introduction of such technologies by telecommunications carriers providing Electronic Mail Services.

Chapter III Registered Agencies for Proper Transmission

Article 14 (Registration of a Registered Agency for Proper Transmission)

The Minister may have a person who is registered by the Minister (hereinafter, the ″registered agency for proper transmission”) conduct the following services (hereinafter, “services for the proper transmission of Specified Electronic Mail, etc.”):

(i) To give instructions or advice to a person who intends to file a petition with the Minister pursuant to the provisions of paragraph (1) or paragraph (2) of Article 8

(ii) To conduct investigations on facts pertaining to the petition in Article 8 paragraph (3), when requested by the Minister.

(iii) To collect and provide information or materials concerning Specified Electronic Mail, etc.

(2) The registration in the preceding paragraph shall be made upon request from a person who intends to conduct the services for the proper transmission of Specified Electronic Mail, etc.

Article 15 (Disqualification)

Any person who falls under any of the following items shall not be registered under paragraph (1) of the preceding article:

(i) Any person who has been sentenced to a fine or severer penalty for a crime stipulated in this Act or an order based upon this Act, provided that a period of two years has not elapsed since the day the sentence was served out or the suspension of such sentence expired

(ii) Any person whose registration was revoked pursuant to the provisions of Article 25, provided that a period of two years has not elapsed since the day of the rescission

(iii) Any juridical person, any of whose officers falls under either of the preceding two items

Article 16 (Criterion for Registration)

The Minister shall grant registration to any person who has applied for registration pursuant to the provisions of Article 14 paragraph (2), if the applicant for registration complies with all of the following items. In this case, the procedures necessary for registration shall be specified in the applicable MIC ordinance.

(i) A person who has graduated from a university, college, or technical college, provided for in the School Education Act (Act No. 26 of 1947) as having mastered subjects concerning telecommunications, and shall have one year or longer of experience in the business of Electronic Mail Services, or a person who has knowledge and experiences equivalent thereto or higher, shall be engaged in the services for the proper transmission of Specified Electronic Mail, etc.

(ii) The following measures shall be taken to properly implement the services for the proper transmission of Specified Electronic Mail, etc.:

(a) A full-time administrator shall be appointed at a unit to implement the services for the proper transmission of Specified Electronic Mail, etc.

(b) Documents shall be prepared to ensure management and proper implementation of the services for the proper transmission of Specified Electronic Mail, etc.

(c) In accordance with the descriptions in the documents under (b), a dedicated unit shall be set up to ensure management and proper implementation of the services for the proper transmission of Specified Electronic Mail, etc.

(2) The registration shall be made by entering the following matters in the registration book of registered agencies for proper transmission:

(i) Date of registration and registration number

(ii) Name and address of the registered agency for proper transmission and, in cases where the person is a juridical person, name of the representative

(iii) Name and address of the office where the registered agency for proper transmission conducts the services for the proper transmission of Specified Electronic Mail, etc.

Article 17 (Renewal of Registration)

The registration under Article 14 paragraph (1) shall, if the registered agency for proper transmission concerned does not renew the registration every three years, lose validity on expiry of the period.

(2) The provisions of Article 14 paragraph (2) and the preceding two articles shall apply, mutatis mutandis, to the renewal of registration under the preceding paragraph.

Article 18 (Obligation Pertaining to Implementation of Services for the Proper Transmission of Specified Electronic Mail, etc.)

Any registered agency for proper transmission shall conduct the services for the proper transmission of Specified Electronic Mail, etc. fairly using methods complying with the requirements listed in each item of Article 16 paragraph (1) and the standards specified in the applicable MIC ordinance.

Article 19 (Notification of Changes)

Any registered agency for proper transmission shall, when intending to change matters listed in item (ii) or item (iii) of Article 16 paragraph (2), notify the Minister to that effect by two weeks prior to the day of said changes.

Article 20 (Operational Rules and Procedures)

Any registered agency for proper transmission shall establish its operational rules and procedures concerning the services for the proper transmission of Specified Electronic Mail, etc. ("operational rules and procedures" in the following paragraph), and shall notify the Minister of the operational rules and procedures prior to the commencement of the services for the proper transmission of Specified Electronic Mail, etc. The same shall apply when such rules and procedures are to be revised.

(2) The operational rules and procedures shall specify the methods of carrying out the services for the proper transmission of Specified Electronic Mail, etc. and other matters specified in the applicable MIC ordinance.

Article 21 (Suspension and Discontinuance of Services)

Any registered agency for proper transmission shall, when intending to suspend in whole or in part or discontinue the services for the proper transmission of Specified Electronic Mail, etc., notify the Minister to that effect in advance, as specified in the applicable MIC ordinance.

Article 22 (Preparation of Financial Statements, etc. and Access, etc. Thereto)

Any registered agency for proper transmission shall, within three months after the end of every business year, prepare a list of properties, a balance sheet and a profit and loss statement or income and expenditure account statement, and a business report (including an electromagnetic record (any record which is produced by electronic, magnetic, or any other means unrecognizable by natural perceptive function, and is used for data processing by a computer;

the same shall apply hereinafter in this article) in cases where electromagnetic records are produced instead of those paper documents; "financial statements, etc." in the following paragraph and Article 38) and retain thereof for a five-year period at its office.

(2) Parties concerned, including a person who has received the Specified Electronic Mail, may, whenever within the business hours of the registered agency for proper transmission, make the following requests. However, when making a request concerning item (ii) or item (iv), the fees set forth by the registered agency for proper transmission shall be paid.

(i) Where financial statements, etc. are written documents, request for access to said documents or copy thereof

(ii) Request for a certified copy or abridged copy of the documents under the preceding item

(iii) Where financial statements, etc. are produced as electromagnetic records, request for access to or copy of matters recorded on said electromagnetic records which are displayed in a manner stipulated in the applicable MIC ordinance

(iv) Request for the matters recorded on electromagnetic records under the preceding item in an electromagnetic manner stipulated in the applicable MIC ordinance or request for delivery of written documents containing said matters

Article 23 (Order for Compliance)

When the Minister deems that the registered agency for proper transmission has failed to comply with any of the items in Article 16 paragraph (1), the Minister may order such registered agency for proper transmission to take the necessary measures for compliance with all such provisions.

Article 24 (Order to Improve Business Activities)

The Minister may, when it is deemed that a registered agency for proper transmission is violating the provisions of Article 18, order the said registered agency for proper transmission to implement the services for the proper transmission of Specified Electronic Mail, etc. pursuant to the provisions of the same article or to take the necessary measures to improve the methods of the services for the proper transmission of Specified Electronic Mail, etc.

Article 25 (Rescission, etc. of Registration)

Where a registered agency for proper transmission falls under any of the following items, the Minister may rescind its registration or order the suspension in whole or in part of its services for the proper transmission of Specified Electronic Mail, etc. for a specified period:

(i) Falls under item (i) or item (iii) of Article 15.

(ii) Violates the provisions of Article 19 through Article 21, Article 22 paragraph (1) or the following article.

(iii) Rejects a request pursuant to the provisions of each item of Article 22 paragraph (2) without justifiable reason.

(iv) Violates the order pursuant to the provisions of the preceding two articles

(v) Obtains the registration under Article 14 paragraph (1) by wrongful means

Article 26 (Maintenance of Record Book)

Any registered agency for proper transmission shall, in accordance with the applicable MIC ordinance, prepare and maintain a record book, in which matters specified in the applicable MIC ordinance related to the services for the proper transmission of Specified Electronic Mail, etc. shall be entered.

Article 27 (Public Notice)

The Minister shall, in the following cases, issue a public notice to that effect in the Official Gazette:

(i) When registering an agency under Article 14 paragraph (1)

(ii) When receiving a notification pursuant to the provisions of Article 19

(iii) When receiving a notification pursuant to the provisions of Article 21

(iv) When rescinding a registration under Article 14 paragraph (1) or ordering the suspension of the services for the proper transmission of Specified Electronic Mail, et

c., pursuant to the provisions of Article 25

Chapter IV Miscellaneous Provisions

Article 28 (Report and On-site Inspection)

Within the limits necessary for the enforcement of this Act, the Minister may order a sender or the consignor of the transmission of Specified Electronic Mail, etc. to report on the state of transmission thereof, or delegate ministerial staff to enter the office of the sender or the consignor of transmission to inspect articles, including record books and documents.

(2) To the extent necessary for ensuring the proper operation of the services for the proper transmission of Specified Electronic Mail, etc., the Minister may order a registered agency for proper transmission to report on the state of the services for the proper transmission of Specified Electronic Mail, etc. or assets, as necessary, or delegate ministerial staff to enter the office of the registered agency for proper transmission to inspect the state of the services for the proper transmission of Specified Electronic Mail, etc., or articles, including record books and documents.

(3) Any ministerial staff who conducts an on-site inspection in accordance with the provisions

of the preceding two paragraphs shall carry an identification card and show it to the persons concerned.

(4) The power of the on-site inspection under the provisions of paragraph (1) or paragraph (2) shall not be construed as being legitimate for the purpose of criminal investigations.

Article 29 (Request to Provide Information on the Sender)

Within the limits necessary for the enforcement of this Act, the Minister may request the telecommunication carrier or other party who has granted the right to use the Electronic Mail Address or codes, including characters, numerical characters and marks (limited to those related to the sender among those displayed on the screen of the communications terminal used by the person receiving Specified Electronic Mails, etc., or those used for receiving and sending of Specified Electronic Mails) to provide information such as the personal name or legal name, address and others that are necessary to identify the person to whom the said right has been granted.

Article 30 (Provision of Information to Foreign Enforcement Authorities)

The Minister may provide any foreign authority that enforces foreign laws and regulations corresponding to this Act (hereinafter, "Foreign Enforcement Authority") with information that is deemed to contribute to the execution of their duties (limited to those corresponding to the duties specified under this Act; the same shall apply in the following paragraph).

(2) As for the provision of information under the preceding paragraph, appropriate measures shall be taken so that the said information will not be used for anything other than execution of the duties of the said Foreign Enforcement Authority, and will not be used for investigation of foreign criminal cases (limited to cases where the target criminal fact has already been identified) or judgment of foreign criminal cases ("investigations" in the following paragraph) unless consent pursuant to the provisions of the following paragraph has been obtained.

(3) The Minister may, upon request from a Foreign Enforcement Authority, give consent for the use of the information provided pursuant to the provisions of paragraph (1) in investigations of a foreign criminal case pertaining to the said request, except for cases that fall under any of the following items:

(i) When the crime that is said to be the target of the investigations of the criminal case pertaining to the said request is a political crime, or when the said request is deemed to have been made with the purpose of performing investigations for a political crime

(ii) If the act relating to the crime that is said to be the target of the investigations of the criminal case pertaining to the said request is assumed to have been conducted in Japan, and when such act is not construed as a crime under the acts and regulations of Japan

(iii) When no guarantee is given by the requesting country to allow Japan to make the same kind of request

(4) The Minister shall, upon giving the consent set forth in the preceding paragraph, receive in advance confirmation from the Minister of Justice that the case does not fall under item (i) and item (ii) of the same paragraph, and confirmation from the Minister for Foreign Affairs that the case does not fall under item (iii) of the same paragraph, respectively.

Article 31 (Administrative Work to Be Conducted by Prefectures)

As specified in the applicable cabinet order, part of the administrative work under the jurisdiction of the Minister stipulated in this Act may be treated as administrative work that shall be conducted by prefectural governors.

Article 32 (Transitional Measures)

When orders should be established, amended or abolished in accordance with the provisions of this Act, necessary transitional measures (including those concerning the Penal Provisions) may be stipulated in those orders to the extent deemed to be reasonably necessary in establishing, amending or abolishing those orders.

Chapter V Penal Provisions

Article 33

Any person who has violated an order to suspend his or her services in accordance with the provisions of Article 25 shall be guilty of an offense and liable to imprisonment with labor for a term not exceeding one year or to a fine not exceeding one million yen, or to both.

Article 34

Any person shall be guilty of an offense and liable to imprisonment with labor for a term not exceeding one year or to a fine not exceeding one million yen in the following cases:

(i) If he or she has violated the provisions of Article 5

(ii) If he or she has violated the order in accordance with the provisions of Article 7 (except those relating to the maintenance of records pursuant to the provisions of Article 3 paragraph (2))

Article 35

Any person shall be guilty of an offense and liable to a fine not exceeding one million yen in the following cases:

(i) If he or she has violated the order pursuant to the provisions of Article 7 (limited to those relating to the maintenance of records pursuant to the provisions of Article 3 paragraph (2))

(ii) If he or she has failed to submit a report pursuant to the provisions of Article 28 paragraph (1), has submitted a false report, or has refused, hindered, or evaded the inspection pursuant to the provisions of the same paragraph

Article 36

Any person shall be guilty of an offense and liable to a fine not exceeding three hundred thousand yen in the following cases:

(i) If he or she has failed to submit a notification or submitted a false notification in accordance with the provisions of Article 21

(ii) If he or she has failed to make entries or made false entries, or failed to maintain records in violation of the provisions of Article 26

(iii) If he or she has failed to submit a report in accordance with the provision of Article 28 paragraph (2), or submitted a false report, or has refused, hindered, or evaded the inspection pursuant to the provisions of the same paragraph

Article 37

When any representative of a juridical person, or any agent, employee, or other staff of a juridical person or a person, has committed an act of violation specified in any of the articles listed below with respect to the business activities of either the juridical person or the person concerned, the violator shall be punished. In addition, the juridical person shall be guilty of an offense and liable to a fine as specified below, and the person concerned shall be guilty of an offense and liable to a fine under the applicable article.

(i) Article 34: A fine not exceeding thirty million yen

(ii) Article 33, Article 35, or the preceding article: A fine under the respective provisions

Article 38

Any person who has failed to retain financial statements, etc., has failed to enter the matters required to be entered in financial statements, etc., or has made false entries in violation of the provisions of Article 22 paragraph (1), or has refused without due reason a request pursuant to the provisions of each item of paragraph (2) of the same article shall be liable to a non-penal fine not exceeding two hundred thousand yen.

Supplementary Provisions

(Effective Date)

(1) This Act shall come into force on the day specified in the applicable cabinet order within six months calculating from the day of promulgation.

(Review)

(2) The government shall, after considering the progress of implementation of this Act in view of the relevant circumstances, including the level of technologies pertaining to telecommunications, take the necessary measures based upon the results thereof within three years calculating from the day of enforcement of this Act.

Supplementary Provisions (Act No. 125 of July 24, 2003) Excerpts

Article 1 (Effective Date)

This Act shall come into force on the day specified in the applicable cabinet order within nine months calculating from the day of promulgation. However, the provisions listed in the following items shall come into force as from the day specified respectively in those items.

(i), (ii) Omitted

(iii) Provisions of Article 2; amended provisions of Article 11 paragraph (2) of the Companies Act in Article 3; and Article 6 through Article 15, Article 21 through Article 31, Article 34 through Article 41, and Article 44 through Article 48 of the Supplementary Provisions: the day specified in the applicable cabinet order within one year calculating from the day of promulgation.

Supplementary Provisions (Act No. 46 of May 20, 2005) Excerpts

Article 1 (Effective Date)

This Act shall come into force on the day specified in the applicable cabinet order within six months calculating from the day of promulgation. However, the provisions in the following article and Article 6 of the Supplementary Provisions shall come into force on the day of promulgation.

Article 2 (Transitional Measures)

A person who wishes to be registered under Article 14 paragraph (1) of the Act on Regulation of the Transmission of Specified Electronic Mail as amended by this Act (hereinafter, the "New Act") may, even before the enforcement of this Act, apply for registration. The same shall apply to the notification of the operational rules and procedures in accordance with the provisions of Article 14 paragraph (1) of the New Act.

Article 3

Any person who is being actually designated, at the time of the enforcement of this Act, under Article 13 paragraph (1) of the Act on Regulation of the Transmission of Specified Electronic Mail before the amendment by this Act (the "Former Act" in the following article), until the day on which six months have elapsed calculating from the day of enforcement of this Act, shall be deemed as being registered under Article 14 paragraph (1) of the New Act.

Article 4

In addition to what is provided for in the preceding article, acts committed prior to the enforcement of this Act, including disposition and procedures, based on the provisions of the Former Act (including orders based on the Former Act), that fall under the provisions of the New Act equivalent to those of the Former Act, shall be deemed as being acts committed, including disposition and procedures, based on the provisions of the New Act.

Article 5 (Transitional Measures Concerning the Penal Provisions)

With respect to the application of the Penal Provisions to any act committed before the enforcement of this Act, the provisions then in force shall still apply.

Article 6 (Delegation to Cabinet Orders)

In addition to the transitional measures specified under Article 2 through the preceding article of the Supplementary Provisions, other transitional measures necessary for the enforcement of this Act (including transitional measures concerning the Penal Provisions) shall be specified in the applicable cabinet order.

Article 7 (Review)

The government shall, after considering the progress of implementation of this Act

in view of the relevant circumstances, including the level of technologies pertaining

to telecommunications, take the necessary measures based upon the results thereof

within three years calculating from the day of enforcement of this Act.

Supplementary Provisions (Act No. 87 of July 26, 2005) Excerpts

This Act shall come into force on the day of enforcement of the Companies Act.

Supplementary Provisions (Act No. 54 of June 6, 2008)

Article 1 (Effective Date)

This Act shall come into force on the day specified in the applicable cabinet order within six months calculating from the day of promulgation. However, the provision of Article 5 of the Supplementary Provisions shall come into force on the day of promulgation.

Article 2 (Transitional Measures Concerning Consent, etc. on the Transmission of

Specified Electronic Mail)

A person who has already notified the sender (the sender specified under Article 2 item (ii) of the Act on Regulation of the Transmission of Specified Electronic Mail after amended by this Act (the “New Act” in this article and the next article); the same shall apply hereinafter in this article) or the consignor of transmission (the consignor of transmission specified under Article 3 paragraph (1) item (i) of the New Act; the same shall apply hereinafter in this article) of the request or the consent to send Specified Electronic Mail (Specified Electronic Mail specified under Article 2 item (ii) of the New Act; the same shall apply hereinafter in this article) at the time of enforcement of this Act shall be deemed as the one listed in Article 3 paragraph (1) item (i) of the New Act.

(2) A person who has already notified the sender or the consignor of transmission of his/her own Electronic Mail Address (Electronic Mail Address specified under Article 2 item (iii) of

the New Act) shall be deemed as the one listed in Article 3 paragraph (1) item (ii) of the New Act.

(3) A notice that has already been given to the sender or the consignor of transmission at the time of enforcement of this Act and that contains a request not to send Specified Electronic Mail (or, in cases where the request was not to send Specified Electronic Mail pertaining to certain matters, the said request) shall be deemed as the notice specified under Article 3 paragraph (3) of the New Act.

Article 3 (Transitional Measures Concerning the Administrative Order)

The order made according to the provisions of Article 7 of the Act on Regulation of the Transmission of Specified Electronic Mail before amended by this Act (the "Former Act" in this article) (limited only to those relating to the provisions of the Former Act equivalent to those of the New Act) shall be deemed as the order made according to the provisions of Article 7 of the New Act.

Article 4 (Transitional Measures Concerning the Penal Provisions)

With respect to the application of the Penal Provisions to any act committed before the enforcement of this Act, the provisions then in force shall still apply.

Article 5 (Delegation to Cabinet Orders)

In addition to the transitional measures specified under the preceding three articles, other transitional measures necessary for the enforcement of this Act (including transitional measures concerning the Penal Provisions) shall be specified in the applicable cabinet order.

Article 6 (Review)

The government shall, after considering the progress of implementation of this Act in view of the relevant circumstances, including the level of technologies pertaining to telecommunications, take the necessary measures based upon the results thereof within three years calculating from the day of enforcement of this Act.

Annex 4. Decree No. 91/2020/ND-CP dated August 14, 2020, on fighting spam messages, spam emails and spam calls (Viet Nam, translated in English)

DECREE

FIGHTING SPAM MESSAGES, SPAM EMAILS AND SPAM CALLS

Pursuant to the Law on Government organization dated June 19, 2015;

Pursuant to the Law on Electronic transaction dated November 29, 2005;

Pursuant to the Law on Information Technology dated June 29, 2006;

Pursuant to the Law on Telecommunications dated November 23, 2009;

Pursuant to the Law on Actions Against Administrative Violations dated June 20, 2012;

Pursuant to the Law on Advertising dated June 21, 2012;

Pursuant to the Law on Cyberinformation Security dated November 19, 2015;

Pursuant to Cybersecurity Law dated June 12, 2018;

At the request of the Minister of Information and Communications;

The Government promulgates a Decree on fighting spam messages, spam emails and spam calls.

Chapter I

GENERAL PROVISIONS

Article 1. Scope

This Decree provides for the fighting of spam messages, spam emails and spam calls; regulations on advertising messages (SMS, MMS, USSD), emails and calls; rights and obligations of organizations and individuals; additional regulations on administrative penalties for sending and making spam messages, spam emails and spam calls.

Article 2. Regulated entities

This Decree applies to organizations and individuals involved in the fight against spam messages, spam emails and spam calls; the sending of advertising messages, emails and making of advertising calls in Vietnam, including:

1. Providers of telecommunications services and/or Internet services.

2. Organization establishing private telecommunications networks.

3. Enterprises and organizations providing emailing services.

4. Senders of advertising messages, emails, and calls (hereinafter referred to as “advertises”)

5. Recipients of advertising messages, emails, and calls (hereinafter referred to as “users”)

6. Relevant organizations and individuals.

Article 3. Definitions

1. Advertising messages, advertising emails, advertising calls are messages, emails and calls that are meant to introduce profitable/non-profitable products and services and their sellers to the public; except news; social policies; personal information; customer service messages of telecommunication enterprises.

2. Customer service messages of telecommunication enterprises are messages sent by telecommunication enterprises to their users to inform them of activities and utilities of the services.

3. Spam messages include:

a) Advertising messages that are sent without users’ prior consent or advertising messages that violate the regulations of this Decree on sending advertising messages;

b) Messages that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

4. Spam emails include:

a) Advertising emails that are sent without users’ prior consent or advertising emails that violate the regulations of this Decree on sending advertising emails;

b) Emails that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

5. Spam calls include:

a) Advertising calls that are made without users' prior consent or advertising calls that violate the regulations of this Decree on making advertising calls;

b) Calls that has prohibited contents specified in Article 9 of the Law on Electronic Transactions, Article 12 of the Law on Information Technology, Article 12 of the Law on Telecommunications, Article 8 of the Law on Advertising, Article 7 of the Law on Cyberinformation Security and Article 8 of the Cybersecurity Law.

6. Blacklists of IP addresses/domains are the lists of IP addresses and domains that are flagged as spamming by certain servers and periodically sent to the Ministry of Information and Communications.

7. "electronic address holder" means the person who creates or is provided with the electronic address.

8. "header" of an email is part of the information of an email that contains information about the sender, recipient(s), routing information, subject and other information about the email.

9. "subject" of an email is part of the header that summarizes the content of the email.

Chapter II

FIGHTING SPAM MESSAGES, SPAM EMAILS AND SPAM CALLS

Section 1. MEASURES FOR FIGHTING AND PREVENTION OF SPAM MESSAGES, SPAM EMAILS AND SPAM CALLS

1. Develop and launch systems for fighting and prevention of spam messages, spam emails and spam calls.

2. Establish criteria for recognition of spam messages, spam emails and spam calls.

3. Carryout surveillance and supervision; share information about sources of spam messages, spam emails and spam calls.

4. Receive and process feedbacks about spam messages, spam emails and spam calls.

5. Supervise the provision of advertising services by messages, emails and calls.

6. Block, revoke electronic addresses that send out spam messages, spam emails and spam calls.

7. Enhance domestic and international cooperation in anti-spam efforts.

8. Spread knowledge and raise awareness of the anti-spam efforts

Article 5. Systems for receiving feedbacks about spam messages, spam emails and spam calls

1. Authority of Information Security (AIS) of the Ministry of Information and Communications shall develop and operate the system for receiving feedbacks about spam messages, spam calls (on 5656 prefix) and spam emails (hereinafter referred to as “anti-spam feedbacks”).

2. When running advertising campaigns, advertisers that send advertising messages shall also send their copies to the system for receiving anti-spam feedbacks mentioned in Clause 1 of this Article.

3. Users of telecommunications, Internet, emailing services may send feedbacks and evidence to the system for receiving anti-spam mentioned in Clause 1 of this Article.

Article 6. Coordinating anti-spam activities

1. Information and data from the system for receiving anti-spam feedbacks and other sources of information and data shall be used for coordinating the prevention and handling of spam messages, spam emails and spam calls.

2. AIS shall coordinate the prevention and handling of spam messages, spam emails and spam calls.

3. Providers of telecommunications, Internet and emailing services and advertisers shall comply with requests of AIS regarding prevention and handling of spam messages, spam emails and spam calls.

Article 7. Do-Not-Call Register

1. Do-Not-Call Register is the list of phone numbers that have been registered by their subscribers who do not want to receive any opt-in message, advertising message or advertising call.

2. Users of telecommunications services are entitled to register or withdraw their legally held phone numbers from the Do-Not-Call Register.

3. Advertisers, providers of telecommunications and Internet services must not make advertising calls, send opt-in messages or advertising messages to any of the phone number on the Do-Not-Call Register.

4. AIS shall organize the development, maintenance, and operation of the Do-Not-Call Register management system; instruct users to subscribe to and unsubscribe from the Do-Not-Call Register; make the list publicly available on the website/web portal of AIS.

Article 8. Blacklist of IP addresses sending spam emails

1. AIS shall organize, develop, and periodically update the blacklist of IP addresses sending spam emails on its website/web portal.

2. Organizations, enterprises and individuals may use this blacklist to block spam emails.

Section 2. RESPONSIBILITIES OF ORGANIZATIONS, ENTERPRISES AND USERS

Article 9. Responsibilities of providers of telecommunications services, Internet services and organizations establishing private telecommunications networks

1. Provide users with instructions on how to fight spam messages and spam calls.

2. Provide users with instructions, tools and applications for reporting and blocking spam messages and spam calls.

3. Strictly implement the measures for prevention of advertising messages and advertising calls to the Do-Not-Call Register mentioned in Clause 1 Article 7 of this Decree.

4. Block and revoke electronic addresses used for sending spam messages, spam emails or making spam calls at the request of competent authorities.

5. Establish and adjust sending frequency limits to detect subscriber numbers suspicious of sending spam messages and improve effectiveness of blocking spam messages according to the nature, scope, and time of blocking spam messages.

6. Establish and operate anti-spam systems that apply artificial intelligence, big data and technological advances.

7. Provide, update, and share samples of spam messages for AIS and other providers of telecommunications services.

8. Establish and connect their brandname management systems to the National Brandname Management System; prevent advertisers from sending messages using the brandnames that are not issued by AIS.

9. Retain subscribing messages, unsubscribing requests, and confirmations of unsubscribing from users after the send these messages through the system of the telecommunications service provider for at least 01 year.

10. Compile, update and share blacklists of IP addresses/domains sending spam emails with AIS and other providers of telecommunications and/or Internet services.

11. Implement measures for fighting and preventing spam messages and spam calls using the criteria for recognition of spam messages and spam calls.

12. Filter IP addresses/domains that send or are used to send spam emails under their management.

13. Cooperate with advertisers, domestic and international providers of telecommunications and Internet services in preventing spam messages, spam emails and spam calls.

14. Implement various measures to evaluate the seriousness of spam messages and spam calls on their telecommunications networks; prepare periodic reports and statistics as instructed by AIS.

15. Do not collect charges for:

a) Unsubscribing requests sent by users;

b) Erroneous advertising messages;

c) Messages whose contents and charges are different from those announced by the advertisers.

16. Prepare periodic reports and statistics as prescribed by competent authorities.

Article 10. Responsibilities of providers of emailing services

1. Provide users with instructions how to fight spam emails.

2. Provide users with instructions, tools and applications for reporting and blocking spam emails.

3. Implement measures to block, filter, update sources of spam emails; have solutions to prevent loss and accidental blocking of users' email addresses.

4. Monitor, inspect and scan their emailing servers to make sure they are not on the sources of spam emails.

5. Implement measures for fighting and preventing spam emails using the criteria for recognition of spam emails.

6. Retain the titles of emails for at least 180 days to serve settlement of advertising email complaints (if any).

7. Prepare periodic reports and statistics as prescribed by competent authorities.

Article 11. Responsibilities of advertisers

1. Check the Do-Not-Call Register mentioned in Clause 1 Article 7 of this Decree to avoid sending opt-in messages, advertising messages, and making advertising calls to the numbers on the Register.

2. Only send advertising messages, advertising emails and make advertising calls to users that have given their prior consent by:

a) Agreeing to receive advertising messages after the advertiser sends the first and only opt-in message;

b) Completing the form and making a confirmation on paper or on the website/web portal, online application or social network of the advertiser;

c) Calling or sending a message to the advertiser's call center to subscribe

d) Using a software program to subscribe.

3. Provide users with tools to access or retain agreements on subscribing to and unsubscribing from advertising messages, advertising emails and advertising calls on their website/web portal to facilitate inspection and complaint settlement.

4. Take responsibility for and verify users' prior consents when sending advertising messages, advertising emails and making advertising calls.

5. Have appropriate solutions and enable users to refuse to receive advertising messages in accordance with Article 16 and advertising emails in accordance with Article 20 of this Decree.

6. Cooperate with providers of telecommunications, Internet, mailing services and relevant organizations in advertising by messaging, emailing, and calling.

7. Retain advertisement subscription requests, unsubscribing requests, and confirmation messages for at least 01 year to facilitate inspection and supervision.

Article 12. Rights and obligations of users

1. Forwards information about spam messages, spam emails and spam calls to the system for receiving anti-spam feedbacks of AIS or that of providers of telecommunications, Internet and emailing services.

2. Decide whether to receive or refuse to receive advertisements.

3. Cooperate with providers of telecommunications, Internet, mailing services, advertisers, and competent authorities in the fight against spam messages, spam emails and spam calls.

Chapter III

ADVERTISING BY MESSAGES, EMAILS AND CALLS

Section 1. REGULATIONS ON ADVERTISING BY MESSAGES, EMAILS AND CALLS

Article 13. Rules for sending advertising messages and advertising emails, making advertising calls

1. Do not send advertising messages or make advertising calls to the numbers on the Do-Not-Call Register mentioned in Clause 1 Article 7 or without prior consents from the users.

2. Advertisers may only send first and only opt-in message to a phone number that is not on the Do-Not-Call Register. The Ministry of Information and Communications shall elaborate regulations on sending opt-in messages.

3. In case the user refuses to receive advertisements or does not answer the first and only opt-in message, the advertiser must not send any additional opt-in message or advertising message to that number.

4. Stop sending advertising messages and advertising emails and making advertising calls to the user after receiving the user's unsubscribing request.

5. Each advertiser may send up to 03 advertising messages to a phone number, up to 03 advertising emails to an email address, and make 01 advertising call to a phone number within 24 hours unless otherwise agreed by the user.

6. Advertising messages may only be sent during 07:00 – 22:00; advertising calls may only be made during 08:00 – 17:00 unless otherwise agreed by the user.

7. Advertisement contents shall be conformable with advertising laws.

8. Only send advertising messages or make advertising calls after a brandname is issued; Do not use phone numbers to send advertising messages or advertising calls.

Article 14. Advertising message requirements

1. Advertising messages shall be tagged in accordance with Article 15 of this Decree.

2. Advertisements of charged services shall specify the charges.

3. Recipients have the option to refuse in accordance with Article 16 of this Decree.

Article 15. Tagging advertising messages

1. All advertising messages shall be tagged.

2. The tag shall be placed at the beginning of the message.

3. The tag shall be [QC] or [AD].

Article 16. Option to unsubscribe from advertising messages

1. The user’s option to unsubscribe from advertising messages shall:

b) be clearly displayed at the end of the advertising message;

b) instruct the user to unsubscribe from advertising messages to which the user previously subscribed;

c) allow the user to reject a specific product or group of products where necessary; and

d) contain clear instructions on how to unsubscribe in the cases specified in Point b and Point c Clause 1 and the unsubscribing methods specified in in Clause 2 of this Article.

2. The unsubscribing request can be made by:

a) sending a message; or

b) making a call.

3. Right after the user's unsubscribing request, the advertiser shall send a confirmation and stop sending the refused type of advertising messages to the user.

4. The confirmation shall:

a) clearly state that the unsubscribing request has been received, time of receipt of the request and stopping sending advertising messages;

b) be successfully sent once and not contain any advertisement.

Article 17. Advertising email requirements

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 in accordance with Article 18 of this Decree.

3. Every advertising email shall contain information about the advertisers in accordance with Article 19 of this Decree.

4. Advertisements of charged services shall specify the charges.

5. Recipients have the unsubscribing option in accordance with Article 20 of this Decree.

Article 18. Tagging advertising emails

1. All advertising emails shall be tagged.

2. The tag shall be placed at the beginning of the email title.

3. The tag shall be [QC] or [AD].

Article 19. Mandatory information about the advertiser in an advertising email

1. Information about the advertiser shall include the advertiser's name, phone number, email address, geographical address, website/web portal, social network (if any).

2. Information about the advertiser shall be clearly displayed and placed right before the unsubscribing option.

Article 20. Option to unsubscribe from advertising emails

1. The user’s option to unsubscribe advertising emails shall:

b) be clearly displayed at the end of the advertising email;

b) contains the statement that the user is entitled to refuse all products from the advertiser;

c) allow the user to reject a specific product or group of products where necessary; and

d) contain clear instructions to unsubscribe in the cases specified in Point b and Point c Clause 1 and the unsubscribing methods specified in in Clause 2 of this Article.

2. The unsubscribing request can be made by:

a) submitting a request on the website, web portal or social network;

b) sending an email; or

c) making a call

3. Right after the user’s unsubscribing request is received, the advertiser shall send a confirmation and stop sending the unsubscribed advertising emails to the user.

4. The confirmation shall:

a) clearly state that the unsubscribing request has been received, time of receipt and stopping sending advertising emails;

b) be successfully sent once and not contain any advertisement.

Article 21. Advertising call requirements

1. All advertising calls shall contain adequate information about the caller (name and address) which is provide before the advertisement contents. Charges shall be specified if charged services are advertised.

2. If the user refuses to receive advertising calls, the advertiser shall promptly stop calling the user.

Section 2. BRAND NAME MANAGEMENT SYSTEM

Article 22. National Brandname Management System

1. National Brandname Management System is a system for management and storage of brandnames nationwide.

2. Every organization and individual may access the National Brandname Management System on tendinhdanh.ais.gov.vn.

3. AIS shall develop and operate the National Brandname Management System.

Article 23. Use of brandnames

1. A brandname used for sending advertising messages or making advertising calls (hereinafter referred to as "brandname") shall consist of up to 11 continuous Latin letters, digits (from 0 to 9), the symbols (-), (_), (.) and spaces and does not discriminate between upper case and lowercase letters; must not contain only digits; is used for displaying or identifying the sender.

2. All organizations and individuals are entitled to register for and use an unlimited number of brandnames for advertising by messaging or calling.

3. A brandname issued by AIS in the National Brandname Management System shall be unique and valid for 03 years from the issuance date/

4. The registration and use of brandnames shall adhere to the principles of equality, non-discrimination, first-come-first served; avoid confusion or misunderstanding caused by homophones and multiple-meaning words or lack of Vietnamese diacritics.

5. The brandname user shall be legally responsible for the purposes of the brandname, accuracy of information and documents in the application.

6. An organization or individual must not use a brandname that is not issued by AIS or that has been issued by AIS to another organization or individual, unless otherwise accepted by the latter; must not violate lawful rights and interests of any other brandname holder.

7. A brandname must not be used after it is revoked.

8. The organization or individual that is issued with a brandname shall pay the issuance and maintenance fee in accordance with regulations of the Ministry of Information and Communications on fees and charges.

Article 24. Application for brandname issuance

An application for brandname issuance shall consist of:

1. If the application is an organization:

a) A certified true copy of the organization's establishment decision or Certificate of Enterprise Registration. In case multiple brandnames are registered under one application, only 01 certified true copy of the Certificate of Enterprise Registration or establishment decision is required;

b) The Brandname Application Form No. 01 enclosed herewith;

c) Relevant documents about intellectual property rights and trademark registration (if any).

2. If the application is an individual:

a) A certified true copy of the ID card or passport;

b) The Brandname Application Form No. 01 enclosed herewith;

c) Relevant documents about intellectual property rights and trademark registration (if any).

Article 25. Submission of the application for brandname issuance

The application for brandname issuance may be submit:

1. by post to AIS; or

2. electronically on tendinhdanh.ais.gov.vn.

Article 26. Issuance of the brandname certificate

1. Right after the application is received, AIS shall send a confirmation email or message to the applicant specifying the date and time of receipt.

2. Within 01 working day from the receipt of the application, AIS shall consider its validity and decide whether to:

a) Issue the brandname and inform the applicant by email or messaging. After the fee has been fully paid by the applicant, AIS shall send the brandname certificate (Form No. 02 enclosed herewith) by email.

b) Reject the applicant and provide explanation by email or messaging, in which case the applicant shall supplement the application and submit it again in accordance with Article 25 of this Decree.

Article 27. Reissuance of the brandname certificate

1. In case any of the information relevant to an issued brandname or the brandname certificate is lost, the holder shall complete and submit the completed Brandname Application Form No. 01 enclosed herewith to AIS in accordance with Article 25 of this Decree.

2. AIS shall reissue the brandname certificate in accordance with Article 26 of this Decree with the same expiry date.

Article 28. Renewal of the brandname certificate

1. Renewal of the brandname certificate means reissuance of the brandname certificate with a new expiry date.

2. At least 15 days before the expiry date, the certificate holder shall complete and submit the completed Brandname Application Form No. 01 enclosed herewith and relevant documents to AIS in accordance with Article 25 of this Decree.

3. AIS shall renew the Brandname Certificate in accordance with Article 26 of this Decree. A brandname may be renewed multiple times. Each renewal shall be 03 years.

Article 29. Revocation of brandname

1. A brandname will be revoked in the following cases:

a) The brandname is used for sending spam messages or making spam calls or providing illegal services as concluded by a competent authority;

b) The brandname maintenance fee is not paid within 30 days from the due date;

c) The brandname has expired and has not been renewed;

d) The revocation is requested by the brandname holder;

e) The revocation is requested by a competent authority.

2. AIS shall send a notification of the revocation to the brandname holder by email or messaging and make an announcement on www.ais.gov.vn.

Section 3. Reporting

Article 30. Reporting

1. Brandname holders shall submit annual reports (Form No. 04 enclosed herewith) or ad hoc reports at the request of AIS.

2. Brandname holders shall submit annual reports according to Form No. 05 enclosed herewith and ad hoc reports at the request of AIS.

3. Telecommunication enterprises that provide messaging services shall submit annual reports according to Form No. 06 enclosed herewith and ad hoc reports at the request of AIS.

Article 31. Reporting time and methods

1. Annual reports shall be submitted before December 31 of the reporting year. An annual report shall contain data obtained during the period from December 15 of the preceding year to December 14 of the reporting year.

2. Soft copies of reports shall be sent to baocaospam@ais.gov.vn and updated on the National Brandname Management System. Instructions on reporting shall be posted on the AIS's website.

Chapter IV

ADMINISTRATIVE PENALTIES

Article 32. Addition of Points c, d, dd to Clause 2; Points p, q, r, s to Clause 4; Points e, g to Clause 6; Point c to Clause 10 of Article 94; Clause 7a to Article 94 of the Government's Decree No. 15/2020/NĐ-CP dated February 03, 2020, on administrative penalties for violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions

"Article 94. Violations against regulations on emails and messages providing product/service-related information"

2. A fine ranging from VND 5,000,000 to VND 10,000,000 shall be imposed for the commission of any of the following violations:

c) Making advertising calls to users without their clear prior consent;

d) Making advertising calls to users who have unsubscribed to advertising calls;

c) Sending opt-in message after the user has refused or does not response.

4. A fine ranging from VND 20,000,000 to VND 30,000,000 shall be imposed for the commission of any of the following violations:

p) Making more than 01 advertising call to 01 phone number within 24 hours unless otherwise agreed by the user;

q) Making advertising calls outside the 08:00 – 17:00 period unless otherwise agreed by the user;

r) Failure to verify users' prior consents when sending advertising messages, advertising emails or making advertising calls;

s) Failure to provide users with tools to access or retain agreements on subscribing and unsubscribing from advertising calls and opt-in messages on the website/web portal to facilitate inspection and complaint settlement.

6. A fine ranging from VND 60,000,000 to VND 80,000,000 shall be imposed for the commission of any of the following violations:

e) Sending opt-in messages against regulations of the Ministry of Information and Communications;

g) Sending an opt-in message to any phone number on the Do-Not-Call Register.

7a. A fine ranging from VND 80,000,000 to VND 100,000,000 shall be imposed for sending advertising messages or making advertising calls to any of the phone number on the Do-Not-Call Register.

10. Remedial measures:

c) Enforced revocation of the phone numbers used for commission of the violations in Point 1 of this Article.".

Article 33. Addition of Points c, d, dd, e to Clause 1; Point e to Clause 2; Points l, m, n, o to Clause 3 of Article 95, Clauses 3a, 3b, 4a to Article 95 of Decree No. 15/2020/NĐ-CP

“Article 95. Violations against regulations on provision of advertising email/message/call services and message-based content services

1. A fine ranging from VND 10,000,000 to VND 20,000,000 shall be imposed for the commission of any of the following violations:

c) Failure to provide tools and applications for users to report and block spam emails themselves;

d) Failure to have measures to block, filter, update sources of spam emails or failure to have solutions to prevent loss and accidental blocking of users’ email addresses;

dd) Failure to monitor, inspect and scan their emailing servers to make sure they are not on the sources of spam emails;

e) Failure to prepare periodic reports and statistics as prescribed by competent authorities.

2. A fine ranging from VND 20,000,000 to VND 30,000,000 shall be imposed for the commission of any of the following violations:

e) Failure to compile, update and share blacklists of IP addresses/domains sending spam emails with AIS and other providers of telecommunications and/or Internet services.

3. A fine ranging from VND 50,000,000 to VND 70,000,000 shall be imposed for the commission of any of the following violations:

l) Failure to provide tools and application for users to report and block spam messages and spam calls themselves;

m) Failure to provide, update and share samples of spam messages with AIS and other providers of telecommunications services;

n) Failure filter IP addresses/domains that send or are used to send spam emails under their management;

o) Failure to evaluate the seriousness of spam messages and spam calls on their telecommunications networks.

3a. A fine ranging from VND 50,000,000 to VND 70,000,000 shall be imposed for use of a brandname that is not issued by Authority of Information Security or that has been issued by AIS to another organization or individual without the latter’s consent; use of a revoked brandname.

3b. A fine ranging from VND 70,000,000 to VND 100,000,000 shall be imposed use of a brandname for sending spam messages or providing illegal services as concluded by a competent authority.

4a. A fine ranging from VND 140,000,000 to VND 170,000,000 shall be imposed for the commission of any of the following violations:

a) Failure to have measures to block advertising messages and advertising calls to the Do-Not-Call Register;

b) Failure to block and revoke electronic addresses used for sending spam messages, spam emails or making spam calls at the request of competent authorities;

c) Failure to develop and operate anti-spam systems;

d) Failure to establish and connect their brandname management system to the National Brandname Management System;

d) Failure to comply with requests of AIS regarding prevention and handling of spam messages, spam emails and spam calls and implementation of other professional measures.".

Article 34. Addition of Points e, g to Clause 2 Article of Decree No. 15/2020/NĐ-CP

"Article 120. Determination of power to impose penalties

2. The People's public security forces:

e) Directors of provincial police authorities shall have the power to impose penalties for the administrative violations in Clause 7a Article 32 of this Decree;

g) The Directors of police departments specialized in high-tech crimes (A05), social order-related crimes (C02), corruption, smuggling, economic crimes (C03), administrative management and social order, drug-related crimes, internal political affairs, economic security shall have the power to impose penalties for the administrative violations in Clause 7a Article 32 of this Decree ."

Chapter V IMPLEMENTATION CLAUSES

Article 35. Effect

1. This Decree comes into force from October 01, 2020.

2. This Decree supersedes the Government's Anti-spam Decree No. 90/2008/NĐ-CP dated August 13, 2008, and the Government's Decree No. 77/2012/NĐ-CP on amendments to Decree No. No. 90/2008/NĐ-CP.

Article 36. Transition clauses

Within 90 days from the effective date of this Decree, telecommunication enterprises shall send electronic documents about declared brandnames to AIS.

Within 180 days from the effective date of this Decree, AID shall publish the list of lawful brandnames according to the documents provided by telecommunication enterprises. Declared brandnames that are not on the list shall undergo the procedures for issuance of new brandnames specified in Articles 24, 25, 26 of this Decree.

Within 90 days from the effective date of this Decree, AIS shall move the system for receiving feedbacks about spam messages from 456 prefix to 5656 prefix.

Article 33 on addition of Clause 3a and Clause 3b to Article 95 of Decree No. 15/2020/NĐ-CP shall be effective on March 01, 2021.

Article 37. Organizing the implementation

1. The Ministry of Information and Communications shall provide guidance on implementation of this Decree within the scope of its functions and power.

2. The Ministry of Public Security shall cooperate with the Ministry of Information and Communications in the fight against unsolicited messages and calls that are meant to commit scam, harassment, spread malicious codes or software or have banned contents prescribed by law.

Article 38. Responsibility for implementation

Ministers, Heads of ministerial-level agencies, Heads of Governmental agencies, Presidents of the People's Committees of provinces, relevant organizations and individuals are responsible for the implementation of this Decree. /