Kingdom of Saudi Arabia
Communication and Information Technology Commission

Public Consultation Document
On the
Anti-SPAM Policy Framework

Rajab 1428 H (July 2007)

1. Introduction

SPAM[1] represents a major annoyance and threat to Internet and communications infrastructure, applications, computer users in general and to users of the Internet in particular.

Many regional and international organizations/bodies/working groups have recognized the problems of SPAM and have taken steps to deal with the problems and issues SPAM causes.

In the Kingdom itself, SPAM has been used for malicious purposes including phishing, spreading viruses and fraud. Currently in the Kingdom there are no regulations that deal with SPAM and its issues directly though, there are different legislative acts that could be indirectly apply to SPAM, such as the Saudi Telecommunications Act, e-transaction act, Anti e-Crime Act etc.

CITC now wishes to establish a suitable policy framework within the Kingdom, to address the issue of SPAM.

The overall objectives of the Anti-SPAM policy framework are to:

- Reduce the transmission of SPAM in the Kingdom
- Ensure that receivers of messages actively consent to receive the messages that are being sent
- Ensure that legitimate message between consenting parties can be transmitted as easily as they can be today
- Ensure that businesses with legitimate products and services are able to continue using electronic messaging service for commerce
- Ensure the Internet and telecommunications related services support the specific cultural and communal values of the Kingdom.

This document presents a list of the key principles to be used in the development of the anti-SPAM policy framework and its corresponding components for the Kingdom of Saudi Arabia.

As part of the development of the anti-SPAM policy framework for the Kingdom of Saudi Arabia, a global benchmarking exercise was conducted to identify leading and best practices. In consultation with CITC, nine countries and eleven international bodies and initiatives were selected to identify the leading and best practices that will be considered for deployment in the Kingdom of Saudi Arabia. Reviews of legislation, regulations and programs were conducted for the following jurisdictions; USA, United Kingdom, Republic of Korea, Australia, Canada, Peru, Malaysia, Belgium, and Singapore. Moreover, detailed review of international bodies who are actively fighting SPAM include: ITU, OECD, WGIG, MAAWG, APWG, APEC TEL Working Group, Seoul Melbourne Anti-SPAM Agreement, London Action Plan, IETF, Mail Service Providers, and SPAMHAUS.

An assessment of the current legislation and regulations in the Kingdom regarding SPAM was conducted and opportunities to enhance regulations addressing SPAM were identified.

As a result, CITC wishes to develop a comprehensive and unified multi-pronged approach to combat SPAM in the Kingdom of Saudi Arabia. The policy framework will take into consideration the following:

[1] Terms used in this document are defined in the Glossary

- The findings of the assessment of the existing Saudi SPAM-relevant legislation;
- The findings of the benchmarking exercise such as the Anti-SPAM policy frameworks adopted by various countries and the recommendations by leading international bodies involved in the fight against SPAM
- Ensuring that the specific religious, communal and cultural aspects of Saudi Arabia are respected.

To initiate the development of this framework, CITC and the project consultant have developed a set of design principles. These principles were based on:

- A thorough assessment of Anti-SPAM leading and best practices in other jurisdictions
- A thorough review of existing legislation and applicable bylaws currently enacted in the Kingdom
- A consultative and iterative review with key CITC subject matter experts, a number relevant government organizations and a number of relevant national companies, the Anti-SPAM Policy framework Working Group and the Steering Committee.

2. Consultation Process

The CITC invites all members of the public, whether in Saudi Arabia or abroad, including private individuals, public organizations, and commercial entities to participate in this consultation process.

The objective of this consultation process is to provide interested parties with the opportunity to provide comments to the CITC on the Anti-SPAM Policy framework principles and to assist the CITC in its decision regarding the approval of the proposed principles in this document.

The draft of the Anti-SPAM Policy framework Principles will be published for Public Consultation.

The CITC invites interested parties to provide detailed comments on any or all decisions. The comments should be supported to the extent possible with relevant rationale, justifications, data, benchmarks and analysis.

In providing the comments, parties are kindly requested, where appropriate, to indicate the section numbers in the document to which their comments relate.

The parties are also kindly requested to specify contact details including the name of the party in addition to the address and phone number(s).

The consultation document and any responses to it are not binding to the CITC. All responses are the property of the CITC.

Responses to this Public Consultation should be submitted to the CITC (in Microsoft Word format) not after 26/09/2007 to either one of the following addresses:

1. E-mail to: SPAMsurvey@citc.gov.sa.

2. Delivery (hard) by hand or by courier to the Office of the Governor.

3. Suggested Anti-SPAM Policy Framework Principles – Lists

You are kindly requested to provide your feedback on the table below containing a listing of the key principles. Participants are kindly requested to review the general principles table below. Consequently, participants are kindly requested to send their feedback to the CITC by following the mechanism explained in the previous section.

For further information regarding each principle, participants can refer to the sections referred to in the last column of the table (Detailed Information Available Under):

Requirements		Principle	Detailed Information Available Under
Regulatory	Consent	The anti-Spam policy framework will support "Implicit" and "Inferred" consent	4.1.1
		Explicit consent will be based upon an "Opt-In" model	
	Technology – Neutral	The definition of SPAM will be technology neutral	4.1.2
	Content of SPAM	The definition of SPAM will only include content having one of the following characteristics: • Unsolicited and commercial • Unsolicited and objectionable	4.1.3
	Bulk or Single Message	The definition of SPAM will be based upon the transmission of a single unsolicited message	4.1.4
	Defining Criteria of SPAM	Based on the previous decisions, the defining criteria of SPAM will be: • Any unsolicited electronic message that contains commercial or objectionable content transmitted without prior consent through electronic communication modes including, but not limited to, e-mails, mobiles short message (SMS), fax, Bluetooth and instant messaging services	4.1.5
	Criteria for legitimate commercial messaging	The defining criteria of legitimate commercial messages will be: • Consent must be obtained prior to transmission • Messages must contain an unsubscribe facility • Messages must contain accurate and fully functional message originators e-mail addresses, telephone numbers and contact information	4.1.6

	SPAM sent from or received in the Kingdom of Saudi Arabia	The Anti-SPAM regulations will apply to all SPAM originating within the Kingdom and Saudi citizens outside of the country transmitting SPAM to recipients within the Kingdom. Taking into account the international nature of SPAM: • The Saudi anti-SPAM regulations applies to SPAM originating from within Saudi Arabia to anywhere in the world • SPAM messages sent by Saudi Arabian citizens outside of Saudi Arabia to recipients within the Kingdom will be governed by the anti-SPAM legislation	4.1.7
	Breadth of Liability	Any individual or organization knowingly benefiting commercially from, or promoting SPAM messages will be held liable	4.1.8
	Exemptions	Saudi Government agencies and statutory bodies will be exempt when transmitting messages for a public purpose or statutory function	4.1.9
	Dictionary Attacks and Address Harvesting Software	The use of dictionary attacks and address harvesting software to facilitate collection or generation of message addresses in any form is prohibited	4.1.10
	Private Right of Action	• Only the regulatory enforcement agency will have the right to sue SPAMmers • Individuals and organizations will have the right to seek legal recourse once they suffer loss or damage	4.1.11
	Privacy	The use of electronic messaging addresses of individuals and organizations in the Kingdom (e-mail, mobile phone, Bluetooth identifiers, fax numbers, IM names, etc) for purposes other than the reason for which it was collected from the relevant people or entities is prohibited	4.1.12
	Sanctions	Sanctions will be imposed for violations of the Anti-SPAM regulations in accordance with the governing legislation	4.1.13
Enforcement	Enforcement jurisdiction distribution	There will be one agency in charge of enforcing the Anti-SPAM regulations	4.2.1
	Nodal Agency – International Issues	There will be one agency in the KSA acting as a single point of contact for all international SPAM related activities	4.2.2
	CERT and ~~Publishing "Black~~ Lists"	CITC's Computer Emergency Response Team (CERT) will publish to ISPs and service providers on a regular basis a	4.2.3

		listing of known addresses transmitting large volumes of SPAM	
	Single Point for SPAM Reporting	There will be one single point of contact for the reporting of all SPAM in the KSA	4.2.4
	Investigative power	The agency responsible for enforcement of the Anti-SPAM regulations will be granted the necessary investigative powers	4.2.5
	Prosecuting	There will be one agency responsible for prosecuting offenders	4.2.6
Industry Driven Initiatives	Binding Codes of Conduct	• SPAM related Codes of Conduct will exist for service providers like ISPs and eMarketers • It is preferred that the Codes of Conduct be made mandatory and binding for relevant service providers • MSPs in the Kingdom will be encouraged to sign the GSMA Code of Conduct	4.3.1
Education and Awareness	Education and Awareness Campaigns	CITC will take responsibility for ensuring ongoing awareness programs will be provided for all stakeholders including end users, businesses, eMarketers, and service providers	4.4.1
SPAM Measurement	SPAM Measurement Program	CITC will ensure that a comprehensive SPAM measurement program will be created and reported on regularly	4.5.1
International Cooperation And Exchange	Participation in Regulatory and Sharing Information Bodies	KSA will participate actively in Anti-SPAM regulatory and sharing information bodies	4.6.1

In addition to the principles listed above, the CITC would like to receive your inputs on the translation of the SPAM term to Arabic. Please refer to the Arabic document for more details.

Please provide your comments.

Suggested Anti-SPAM Policy Framework Principles – Details

The following provides a listing and description of the Anti-SPAM policy framework's principles, by component, which will be used to develop and deploy the comprehensive framework.

4.1 Regulatory

Principles for the legislative portion of the policy framework focus on providing a definition of SPAM include:

4.1.1 Consent

Implicit and Inferred Consent

- The anti-Spam policy framework will support "Implicit" and "Inferred" consent.

Implicit and inferred consent will be assigned to:

- All pre-existing relationships.
- New relationships where the exchange of information via e-mail or other messaging systems is inherent in the relationship, employer, clubs, etc
- Conspicuous publication of electronics addresses, unless otherwise stated.

Please provide your comments.

Explicit Consent – Opt-In

- Explicit consent will be based upon an "Opt-In" model.

There are two models through which explicit consent (approval) can be provided to individuals or organizations wanting to transmit messages.

1. "Opt-In": Receivers of messages must specifically provide the senders of messages with permission to transmit messages to them PRIOR to any messages being sent.
2. "Opt-Out": Receivers of messages need not specifically provide the senders of messages with permission to transmit message to them PRIOR to any messages being sent. Though following the receipt of a message, they may choose to opt out of receiving further messages from the sender, by requesting them not to send any more messages.

In alignment with the dominant international trend[2], the CITC has adopted the Opt-in approach which protects an individual's privacy and right to receive only the message that they asked for. Companies and organizations will be responsible for maintaining up to date listings of individuals who have "opted-in." Companies and organizations must be prepared to be audited periodically and respond quickly when questions concerning the status of an Opt-in are raised.

Please provide your comments.

[2] Countries which are aligned with this best practice include: Canada, Australia, UK, Belgium, Malaysia, Peru and Singapore

4.1.2 Technology –Neutral

- The definition of SPAM will be technology neutral.

There are a variety of messaging technologies that may be misused to send SPAM. Technological developments and convergence may lead to the new messaging media arising or existing ones changing their form and presentation. The legislative definition of SPAM may focus on either:

- A technology-by-technology description, OR
- More generic, technology neutral description.

A technology neutral approach does not specify the technologies, whereas, a technology-by-technology definition is more focused and specifies the applicable technologies such as: email, SMS, MMS, fax, instant messaging, voice mail, automated calling machines, etc.

Although some of the existing legislative best practices around the globe[3] are Technology specific, the CITC has chosen the technology-neutral approach to define SPAM in alignment with the existing CITC policies and practices.

Please provide your comments.

4.1.3 Content of SPAM

- The definition of SPAM will only include content having one of the following characteristics:
  - Unsolicited and commercial.
  - Unsolicited and objectionable.
- The definition of SPAM will not include content that is unsolicited and non-commercial. For example, unobjectionable religious, unobjectionable political, etc.

Unsolicited electronic messages can be of varying content. The content could be commercial, political, religious or objectionable in nature. In alignment with common international practices[4] only objectionable messages (as defined in the Anti e-Crime Act) or commercial messages "which promote a product or service for financial gain" be considered SPAM. The content of objectionable, malicious or criminal messages is addressed in the Kingdom by the Anti e-Crime Act. The vast majority of SPAM transmitted today around the world and in Saudi Arabia is commercial in nature, it directly or indirectly promotes products and services for financial gain that may be legitimate or in fact fraudulent. This approach will address the vast majority of the SPAM being transmitted, simplify investigation and ensure the effort of regulation and prosecution where required is reasonable.

Please provide your comments.

[3] Countries which are aligned with this best practice include: USA, Republic of Korea, Canada, Australia, UK, Belgium, etc
[4] Countries which are aligned with this best practice include: USA, Republic of Korea, Canada, Australia, UK, Belgium, Malaysia, Peru and Singapore.

4.1.4 Bulk or Single Message

- The definition of SPAM will be based upon the transmission of a single unsolicited message

SPAM sent in bulk is defined as when the sender distributes a large number of the same message to unsolicited or / unconsenting recipients. Leading practices in other jurisdiction's policy frameworks[5] stipulate that even a single unsolicited message can be considered to be SPAM if the other defining criteria are met.

In view of international leading practices the increased simplicity of identification and investigation associated with determining if is a message is SPAM, CITC has determined that even one unsolicited message will be treated as SPAM if the other defining criteria are met.

Please provide your comments.

4.1.5 Defining Criteria of SPAM

Based on the previous decisions, the defining criteria of SPAM will be:

- Any unsolicited electronic message that contains commercial or objectionable content transmitted without prior consent through electronic communication modes including, but not limited to, e-mails, mobiles short message (SMS), fax, Bluetooth and instant messaging services.

Having a clear SPAM definition will simplify the identification, enforcement and compliance activities of individuals, companies, service providers and regulators

As previously discussed in previous sections (3.1.1, 3.1.2, 3.1.3, 3.1.4), CITC has defined SPAM as:

- Any unsolicited commercial or objectionable message received;
- Regardless of the volume transmitted; and
- Sent through electronic communication modes including, but not limited to, e-mails, mobiles short message (SMS), fax, Bluetooth and instant messaging.

Based on these decisions, CITC has simplified the precise definition of SPAM. It consists of the following three distinctive features:

1. SPAM is unsolicited (regardless of the content and number of messages being sent); and
2. SPAM's content is commercial or objectionable in nature
3. SPAM is transmitted via electronic communication modes including, but not limited to, e-mails, mobiles short message (SMS), fax, Bluetooth and instant messaging.

Please provide your comments.

[5] Countries which are aligned with this best practice include: Single message can be considered as SPAM: Republic of Korea, Canada, Australia, UK, Belgium, Malaysia, Peru.

4.1.6 Criteria for Legitimate Commercial Messaging

The defining criteria of legitimate commercial messages will be:

- Consent must be obtained prior to transmission.
- Messages must contain an effective and easy to use unsubscribe facility.
- Messages must contain accurate and fully functional message originators e-mail addresses, telephone numbers and contact information.

To preserve the inherent utility of the messaging mediums being misused to transmit SPAM, the Saudi anti-SPAM policy framework and corresponding regulations will define the requirements that constitute transmission of a legitimate message.

The requirements for determining if the transmission of electronic messages are legitimate are as follows:

1. Consent must be obtained before sending commercial messages, explicit, implicit or inferred.
2. Every electronic commercial message that offers or promotes, services, products must contain a functioning and free of charge unsubscribe facility, enabling the recipient to unsubscribe from further electronic messages.
3. Every electronic commercial message must contain an accurate and functional e-mail address or a telephone number, by which the sender can be readily contacted.

Please provide your comments.

4.1.7 SPAM Sent From or Received in the Kingdom of Saudi Arabia

- The Anti-SPAM regulations will apply to all SPAM originating within the Kingdom and Saudi citizens outside of the country transmitting SPAM to recipients within the Kingdom.

Taking into account the international nature of SPAM:

1. The Saudi anti-SPAM regulations applies to SPAM originating from within Saudi Arabia to anywhere in the world.
2. SPAM messages sent by Saudi Arabian citizens outside of Saudi Arabia to recipients within the Kingdom will be governed by the anti-SPAM legislation.

Note, SPAM originating outside on the Kingdom, transmitted by non-Saudi citizens will be addressed through intentional agreements and working groups.

Please provide your comments.

4.1.8 Breadth of Liability

- Any individual or organization knowingly benefiting commercially from, or promoting SPAM messages will be held liable and will be prosecuted under the Anti-SPAM regulations.

To prevent businesses from hiding behind individual senders of SPAM, to ensure fully\ legal action can be pursued against all the beneficiaries of SPAM, and in alignment with best practices and global anti-SPAM regimes, [6] CITC has decided that in addition to the sender of the SPAM messenger, any other person or organization knowingly benefiting from or promoting SPAM messages will also be liable.

Please provide your comments.

4.1.9 Exemptions

- Saudi Government agencies and statutory bodies will be exempt when transmitting messages for a public purpose or statutory function.

Prohibiting the transmission of SPAM messages does not preclude all types of unsolicited messages to be sent. Saudi anti-SPAM regulations will exclude electronic messages which are sent with the authority of the Saudi Government or a statutory body for a public purpose or statutory function. Other exemptions will be added to the by-laws as required.

Please provide your comments.

4.1.10 Dictionary Attacks and Address Harvesting Software

- The use of dictionary attacks and address harvesting software to facilitate collection or generation of message addresses in any form is prohibited.

In order to facilitate the reduction of SPAM the Saudi anti-SPAM regulations will prohibit:

- Supplying, acquiring or using of Address-harvesting software;
- Supplying, acquiring or using an electronic address list produced using address-harvesting software; and
- Sending of electronic messages to users through the use of a dictionary attack or address harvesting software.

Please provide your comments.

4.1.11 Private Right of Action

- Only the regulatory enforcement agency will have the right to sue SPAMmers
- Individuals and organizations will have the right to seek legal recourse once they suffer loss or damage.

There will be no private right of action for any individual or organization other than the regulatory enforcement agency while preserving the right of individuals and organizations to seek legal recourse. This approach recognises that:

- It would not be cost-effective for individuals and / or small business to institute legal action, let alone having sufficient resources to gather additional evidence in order to institute legal action;

[6] Countries which are aligned with this best practice include: USA, Canada, Australia, UK, Belgium, Malaysia, etc.

- SPAM almost always affects more then one individual or organization thus when warranted efficiencies in prosecution and penalties can be achieved;
- Legal processes will not become burdened with a large number of cases and plaintiffs seeking recourse; and
- The enforcement agency can prioritize and focus resources on key offenders and situations.

Please provide your comments.

4.1.12 Privacy

- The use of electronic messaging addresses of individuals and organizations in the Kingdom (e-mail, mobile phone, Bluetooth identifiers, fax numbers, IM names, etc) for purposes other than the reason for which it was collected from the relevant people or entities is prohibited.

In alignment with the existing privacy-related regulations of the Kingdom, the transmission of any SPAM message that adversely impacts the privacy of an individual or organization in the Kingdom is prohibited. Misuse of messaging addresses and phone numbers includes:

- The unapproved use;
- Use for purposes not intended or approved;
- The gather of message addresses or phone numbers with intention to sell; and
- The purchase of collected messaging addresses or phone numbers.

Please provide your comments.

4.1.13 Sanctions

- Sanctions will be imposed for violations of the Anti-SPAM regulations in accordance with the governing legislation.

Applying sanctions is crucial, if SPAM transmissions are to be effectively curbed. Sanctions will be imposed for violations of the Anti-SPAM regulations in accordance with the governing legislation. Other sanctions maybe imposed based on the content of the message, for example objectionable message content is defined and enforced under the Anti e-Crime Act.

Please provide your comments.

4.2 Enforcement

4.2.1 Enforcement Jurisdiction Distribution

- There will be one agency in charge of enforcing the Anti-SPAM regulations.

There will be one agency in charge of enforcing the SPAM regulations. The agency selected will be based on the legislative framework selected.

Please provide your comments.

4.2.2 Nodal Agency - International Issues

- There will be one agency in the KSA acting as a single point of contact and coordination for all international SPAM related activities.

To ensure robust enforcement, and in accordance with best practices, [7] there will be one agency within the Kingdom assigned as a coordinator to serve as single the point of contact to deal with SPAM issues and activities at the international level.

Please provide your comments.

4.2.3 CERT and Publishing "Black Lists"

- CITC's Computer Emergency Response Team (CERT) will publish to ISPs and service providers on a regular basis a listing of known addresses transmitting large volumes of SPAM.

Essential to reducing the volumes of SPAM will be coordination between CITC and ISPs in blocking SPAM from known offenders both nationally and internationally. To aid in this process CITC's CERT will publish regularly to all licensed providers a listing of known addresses for these offenders so that these SPAM transmission can be stopped.

Please provide your comments.

4.2.4 Single Point for SPAM Reporting

- There will be one single point of contact for the reporting of all SPAM in the KSA.

To facilitate the reporting process and to avoid confusing the SPAM victims, a single point of reporting for SPAM in the Kingdom will be established.

Please provide your comments.

[7] Even where there are multiple agencies involved in the enforcement process, there is always one nodal agency that takes the role of coordinator and acts as a point of contact with the globe.

4.2.5 Investigative power

- The agency responsible for enforcement of the Anti-SPAM regulations will be granted the necessary investigative powers.

The power to conduct investigations and gather information and evidence is a critical for effective enforcement of the regulations. Accordingly the Saudi enforcement authority responsible for enforcement of the SPAM regulations will be granted sufficient investigative power in order to preserve, access, intercept, search and seize electronic evidence.

Please provide your comments.

4.2.6 Prosecuting

- There will be one agency responsible for prosecuting offenders.

There will be one agency in charge of prosecuting offenders of the SPAM regulations. The agency selected will be based on the legislative framework selected.

Please provide your comments.

4.3 Industry Driven Activities

4.3.1 Binding Codes of Conduct

- SPAM related Codes of Conduct will exist for service providers like ISPs and eMarketers.
- It is preferred that the Codes of Conduct be made mandatory and binding for relevant service providers.
- MSPs in the Kingdom will be encouraged to sign the GSMA Code of Conduct.

To encourage co-regulation, SPAM related codes of Conduct will exist for service providers like ISPs and eMarketers. It is preferred these codes of conduct be made mandatory and binding. As there is already the GSMA code of conduct in place, MSPs will be encouraged to sign it.

Please provide your comments.

4.4 Education and Awareness

4.4.1 Education and Awareness Campaigns

- CITC will take responsibility for ensuring ongoing awareness programs will be provided for all stakeholders including end users, businesses, eMarketers, and service providers.

Increasing education and awareness is a crucial part of a comprehensive anti-SPAM strategy. Therefore, ongoing awareness programs will be run by the regulatory agency for all stakeholders including end users, businesses, eMarketers, and service providers.

Please provide your comments.

4.5 SPAM Measurement

4.5.1 SPAM Measurement Program

- CITC will ensure that a comprehensive SPAM measurement program will be created and reported on regularly.

The measurement SPAM is critical to understanding the effectiveness of the anti-SPAM solutions being deployed to reduce SPAM. A comprehensive SPAM measurement program will be created and reported upon on a regular basis to all stakeholders.

Please provide your comments.

4.6 International Cooperation And Exchange

4.6.1 Participation in Regulatory and Sharing Information Bodies

- KSA will cooperate and participate actively in Anti-SPAM regulatory and sharing information bodies.

In alignment with the international trend and the best practices recommendations, KSA will be participating internationally at the regulatory level entering into MoUs, belonging to international bodies fighting against SPAM. The Kingdom will also participate in information sharing bodies and initiatives focused on sharing knowledge, raising awareness, developing international codes and guidelines, and promoting best practices.

Please provide your comments.

4. Glossary

No.	Acronym	Meaning
1.	APEC	Asia-Pacific Economic Cooperation Telecommunications & Information Working Group (APEC)
2.	APWG	The Anti-Phishing Working Group (APWG)
3.	CITC	Communications and Information Technology Commission;
4.	Ancillary elements	The activities that might be conducted before sending SPAM. Examples are address harvesting (collecting email addresses) and dictionary attacks (randomly generating email addresses);
5.	Bulk	Spam messages that are typically sent in large numbers in an indiscriminate manner, without any knowledge about the recipient other than the e-mail address;
6.	Computer service	Includes computer time, data processing and the storage or retrieval of data;
7.	Consent	Is the permission that legislators or regulators wish to require from the sender before sending messages;
8.	Damage	It is the quantifiable amount of damage measured as a consequence of the SPAMming action;
9.	Dictionary attacks	Addresses are automatically generated based on words from a dictionary, common names and numbers;
10.	Email Client	An email client is a client side application (program) that is used by the email sender(s) to primarily compose and send emails and used by the email receiver(s) to primarily retrieve and view emails;
11.	Email Server	Is a server side application (program) that interacts with email clients and other email servers as well. It runs on a server computer to specifically receive emails from email clients and send them through the network as well as to receive emails through the network and deliver them to the email clients;
12.	Explicit consent	Form of consent where an individual or organization has actively given their permission to a particular action or activity (opt-in);
13.	EY	Ernst & Young;
14.	Function	Includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;
15.	Governor	Governor of Communications and Information Technology commission;
16.	Headers	Headers are the part of an email that most people do not see. Headers contain not only the "Subject:" line, but a complete list of the path that the email took along various machines on the Internet to reach its destination. Learning to decipher headers is a major part of becoming a spam hunter, because the spammer will usually try to forge, conceal, and mislead with the headers;
17.	IETF	The Internet Engineering Task Force (IETF)
18.	Implicit/Inferred consent	Consent which generally can be inferred from the conduct and/or other business relationships of the recipient

No.	Acronym	Meaning
19.	Information Network / Internet	Network connection between more than one information system to obtain or exchange information;
20.	Information System	Software packages or tools prepared to process and manage data;
21.	Intercept	In relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;
22.	ITU	The International Telecommunication Unions
23.	LAP	London Action Plan: An international action plan designed to encourage communication and cooperation between countries in tackling spam and spam-related problems
24.	Liability	Define who is responsible for SPAM offences. Moreover, laws may address secondary liability, such as for those who encourage violations of spam laws, produce software that creates and transmits messages, or create tools to compile addresses by searching locations such as Internet news groups or by creating them through combinations of letters and numbers;
25.	MAAWG	Messaging Anti-Abuse Working Group (MAAWG)
26.	Message Originator	Has the meaning given to it in section B, subclause 1.2.2 and includes any individual or Organisation (including sole traders and partnerships) that sends or causes to be sent and authorises the sending of Commercial Communications to promote, advertise or offer to supply its own products or services, where the Use of Commercial Communications is the sole or principal means of promoting, advertising or offering to supply its own products and services.
27.	Message Service Provider	Has the meaning given to it in section B, subclause 1.2.3 and includes any individual or Organisation (including sole traders and partnerships) which, by contract or other arrangement (other than a contract of employment) sends or causes to be a sent a Commercial Communication on behalf of a Message Originator or Message Authoriser.
28.	MMS	Is a standard for telephony messaging systems that allows sending messages that include multimedia objects (images, audio, video, rich text) and not just text as in SMS;
29.	OECD	The Organization for Economic Co-operation and Development
30.	Regulator	Is the entity in charge of enacting and enforcing the anti-SPAM related laws in Saudi Arabia;
31.	Right to recourse	The right given to entities to pursue spammers in the court of law;

No.	Acronym	Meaning
32.	Sanctions	Are penalties imposed on SPAMmers by the authorized agencies in case of any breach of the SPAM related laws;
33.	Short Message Service (SMS)	Is a service provided by service providers specialized in licensed public telecommunication services in the Kingdom. This service allows service providers or their customers to send or exchange short (text, audio or video) messages. These messages may be addressed directly to the customer, or it can be a public message aired over a certain area to promote a certain product, to provide customers with certain information or to notify them of new developments. It can also be used for to replying to customers' inquiries and other similar services. The messages can be up to 160 characters;
34.	Site	A site where information are made available on the internet through a specific address (URL);
35.	Software	Data that includes guidelines or applications, when operated in computer, it will perform the required function;
36.	Spam metrics	The metrics allow the evaluation of national strategies and their implementation and provide insights into what changes are needed in policy, regulatory and technical frameworks;
37.	Spammer	The one who sends SPAMs.
38.	Technology Neutral	The regulatory instrument covers communication technologies in general, and is sufficiently flexible to encompass future changes in messaging technology without needing amendment;
39.	Technology Specific	Target specific messaging technologies, such as email, SMS, etc.
40.	WGIG	Working Group on Internet Governance (WGIG)