

Communication and Information Technology Commission

REVIEW OF CURRENT LEGISLATIONS AND SELECTED LEGAL CASES

Final Version

19/09/2007

Submitted to:

Submitted By:



Acceptance of Deliverable

Name	
Title	
Role	
Signature	
Date	



Table of Contents

1	Purpose	5
1.1	Approach used.....	5
2	Executive summary.....	6
3	Identification of legal domains	8
3.1	Relevant legal domains.....	9
4	Assessment of the Relevant Legislations in the Kingdom.....	11
4.1	The Telecom Act and its Bylaws.....	11
4.2	The Monetary and Banking Laws and Regulations.....	20
4.3	Anti-Commercial Fraud Law	22
4.4	Electronic Transactions Act	22
4.5	Anti e-Crime Act.....	23
4.6	Conclusion.....	24
5	Review of Legal cases	28
5.1	Approach Used	28
5.2	Case-1: Email SPAM case by Microsoft against Sahara.....	28
5.3	Case-2: Mobile SPAM	30
5.4	Case-3: Mobile SPAM – 700 Numbers.....	33
5.5	Conclusion.....	34
6	Appendix A: Anti e-Crime Act.....	35
7	Appendix B: eTransactions Law – Draft Version.....	39
8	Appendix C: Telecommunications Act.....	51



1 PURPOSE

Generally speaking, unsolicited¹ bulk² messages and communications containing commercial, abusive or objectionable content and which are sent to people or individuals without their consent by email, fax, or instant messages such as SMS are considered to be SPAM. Several variants of this definition have been adopted in other countries. For instance, in Australia, SPAM does not have to be bulk in nature and even a single unsolicited commercial electronic message could be considered to be SPAM.

Many regional and international organizations/bodies/working groups/initiatives such as WSIS (World Summit on Information Society), ITU, OECD, WGIG (Working Group on Internet Governance), APEC TEL Working Group, ACMA, CNSA, APWG (Anti-Phishing Working Group), MAAWG (Messaging Anti-Abuse Working Group), UNCTAD (United Nations Conference on Trade and Development), IESG (Internet Engineering Steering Group) who publish anti-SPAM RFCs, and selected international agreements such as the “London Action Plan on International SPAM Enforcement Cooperation” (2004), have taken steps to deal with the issue of SPAM.

In the Kingdom of Saudi Arabia as well, SPAM has been used for phishing, spreading viruses and fraud. No specific regulation has been issued to deal with SPAM in the Kingdom of Saudi Arabia; though other existing legislations and regulations, such as the Telecom Act or the Anti e-Crime Act in the Kingdom, could indirectly apply to SPAM.

As the Telecom and IT regulatory authority in Saudi Arabia, the Communications and IT Commission (CITC) now plans to develop a suitable framework in the Kingdom of Saudi Arabia, to address the issue of SPAM.

This assessment of Anti-SPAM regulations in Saudi Arabia has been developed to help identify how the issue of SPAM is currently being addressed by the existing Saudi legislations.

The SPAM definition used in this document will be used for the sole purpose of this document, until a formal definition of SPAM is agreed upon in the Kingdom of Saudi Arabia.

1.1 APPROACH USED

Our approach to meet the objective of this exercise was based on identification of relevant legislations to be reviewed initially, and then considering these legislations from the perspective of the broad control requirements to address SPAM, as well as the elements in the regulatory framework recommended by OECD in this regard.

¹ electronic messages that are not requested by the recipient and are of an advertising or promotional nature

² Messages that are sent in numbers exceeding a predefined threshold in a predefined period of time

Final Version	Page 5 of 64 Confidential - Internal Use Only	
----------------------	--	--



2 EXECUTIVE SUMMARY

SPAM represents a major annoyance and threat to ICT applications users in general and to Internet users in particular. Until recently, internet users were the largest segment of any society to be affected by SPAM. Now SPAM is spreading into all means of communications like mobile phones, facsimile transmissions, and SPAMmers are always on high-alert to exploit any new technology in order for them to achieve their goals. Many countries, regional and international organizations/bodies/working groups/initiatives have taken steps to deal with the issue of SPAM.

In the Kingdom of Saudi Arabia, SPAM has been reportedly used for phishing, spreading viruses and fraud. Currently, there is no formal framework in place to explicitly deal with the issue in the Kingdom of Saudi Arabia; though, there are different legislations and regulations, such as the Saudi Telecom Act and the Anti e-Crime Act that could indirectly apply to SPAM.

Since the development of anti-SPAM legislative guidelines that tackles SPAM is fundamental, the Telecom and IT regulatory authority in Saudi Arabia, the Communications and IT Commission (CITC), plans to develop a suitable framework in the Kingdom of Saudi Arabia, to address the issue of SPAM. Hence, this report assesses the Anti-SPAM regulations in Saudi Arabia and identifies how the issue of SPAM is currently being addressed by the existing Saudi legislations.

The assessment was based on consideration of the adequacy of the relevant legislations in Saudi Arabia, as well as benchmarking it against the elements in the regulatory framework recommended by OECD in this regard. Moreover, selected recent SPAM related complaints and legal cases were analyzed to further understand the gaps in the current Anti-SPAM related legislations.

Currently, no Anti-SPAM legislation exists in Saudi Arabia. In order to focus the review on the most relevant legislations, the SPAM Activity Life-Cycle developed for use as a reference framework during the study, was used to identify the most relevant legislations. Key legislations identified as being of relevance in this context were³:

- The Privacy/Data Protection domain, since the issue of consent as well as protection of eMail addresses and mobile numbers is central to the Privacy domain,
- The Telecom domain, specifically in the context of the Telecom Act, its Bylaws, and the licensing requirements of the various service providers, which is relevant in the context of the control it exerts on the media or carriage providers to the SPAMmers,
- The commercial domain, in the context of consumer protection regulations where, according to the anti-commercial fraud law, the Ministry of Commerce (MOC) will be in charge of enforcing this law,
- The Banking domain, specifically in the context of the Banking Act which falls under the responsibility of SAMA and the Phishing related issues in the Kingdom caused by SPAM, and
- The IT domain, specifically in the context of the e-Transactions Act and the e-Crimes Law.

Provisions in these legislations were also reviewed against provisions recommended by bodies like OECD and ITU.

Having reviewed the stated laws in the Kingdom, it was considered that while legislations like Telecom Act provided certain controls on the privacy of information related to telecom service

³ The Anti e-Crime Act and Electronic Transactions law, please refer to Appendix A and B. For detailed information about other laws and licenses, please refer to CITC Web site at <http://www.citc.gov.sa>.

Final Version	Page 6 of 64 Confidential - Internal Use Only	
---------------	--	--



subscribers, no universal privacy law existed in the Kingdom that ensure that data was used only for the purpose for which it was provided. While the existing Telecom Act and associated licensing agreements do provide for privacy requirements, the lack of a suitable audit mechanism appears to have resulted in weak enforcement.

While the existing Telecom Law, and its Bylaws, provide a good basis for the control of telecommunication service providers in the Kingdom, neither it nor its Bylaws address SPAM fully. SPAM has not been clearly defined in any of the existing legislations. While the Anti e-Crime Act prohibits certain type of content in electronic messages, it does not explicitly address the issue of unsolicited commercial messages, considered to be a major form of SPAM.

Although licensing agreements exist with ISPs, Bluetooth message providers and Bulk SMS Service Providers, significant gaps exist in the ability of the existing terms and conditions to address SPAM effectively.

The anti-commercial fraud law and the Anti e-Crime Act establish a suitable basis for prosecution of SPAMmers involved in publishing illegal content, including misleading and fraudulent advertisements, pornographic and sexual content as well as content that breach the privacy of other individuals in the Kingdom. However, as mentioned earlier, significant gaps exist in the Anti e-Crime Act ability to address SPAM since it does not, for instance, explicitly define SPAM and unsolicited commercial advertisements, nature of consent required, and requirements for legitimate messaging.

While SAMA does provide Internet Banking Security guidelines, there are no explicit instructions published as yet on the manner in which Phishing related issues need to be addressed by the Banks, both in terms of user education and awareness, as well as reporting Phishing cases. Indeed, a formal procedure for reporting Phishing complaints is being developed currently in conjunction with the Banks as are user education and awareness guidelines.

It is also considered that weaknesses in the Anti e-Crime Act enforcement mechanism, resulting from the lack of formal coordination mechanisms between MOI and CITC and the absence of IT Crime investigation specialists, could limit the effectiveness of addressing Phishing crimes.

Having also considered the existing legislations in the context of the regulatory elements recommended by OECD, it is obvious that the current regulatory framework in Saudi Arabia falls behind the key requirements recommended by OECD.

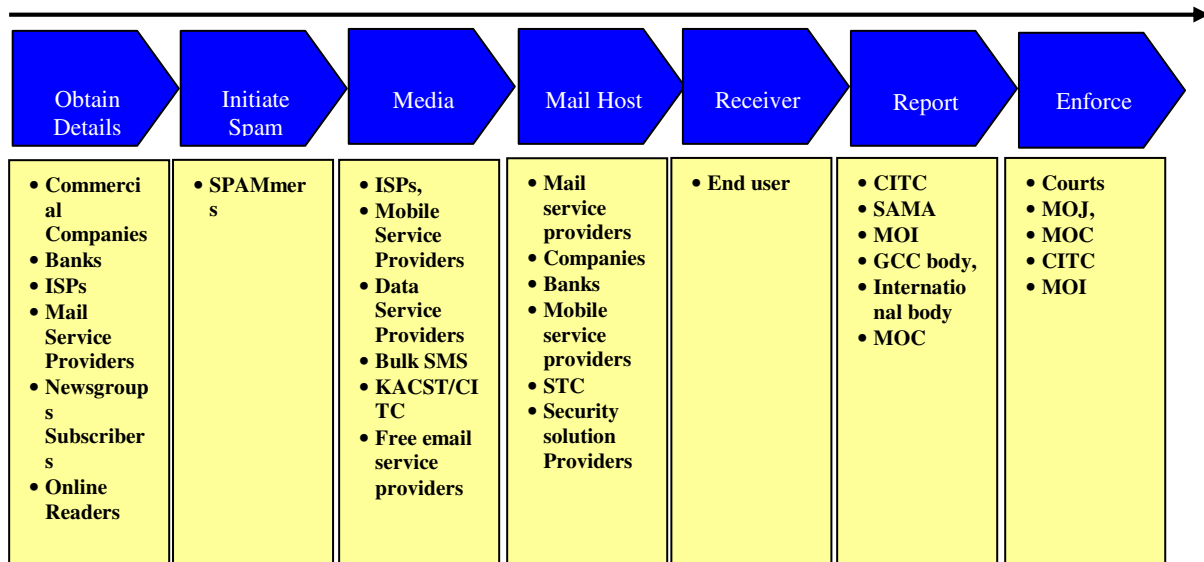
To further understand the gaps, three SPAM related complaints/cases, provided by CITC, were analyzed. The analysis of these cases indicate that the lack of a formal framework to address SPAM had resulted in none of the cases being prosecuted in a court of justice and accordingly, no penal action was taken against the perpetrators.

In conclusion, while the existing legislations in Saudi Arabia do address SPAM in certain aspects, it is evident that significant gaps still exist in the legislative framework that still needs to be addressed. The three cases highlight the importance of being able to address SPAM through a well-defined policy framework that encompasses regulations, international agreements, well-defined enforcement mechanisms, and industry initiatives.



3 IDENTIFICATION OF LEGAL DOMAINS

In an earlier document, we had identified the key stakeholder groups involved with either initiating or dealing with SPAM, by reviewing the SPAM Activity Lifecycle. These stakeholder groups are shown in the figure below.



In order to effectively address SPAM within the Kingdom, ideally there should be suitable guidelines that impose suitable controls on each stage of the SPAM Activity Lifecycle, not just at the last stage to support the prosecution of the SPAM offenders, through a SPAM Act.

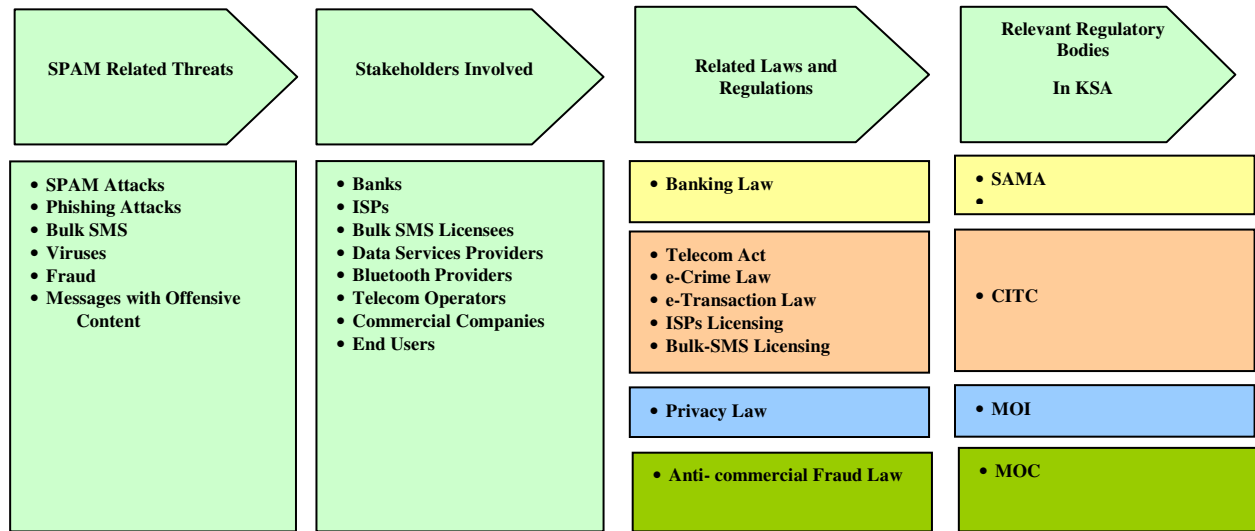
Accordingly, we consider it important to consider the availability in the Kingdom of:

1. A suitable Privacy or Data Protection Act, which ensures that personal information obtained by various organizations in the first stage of the SPAM Activity Lifecycle, are used only for the purpose that it was obtained. Thus, organizations are barred from using these personal details for eMarketing purposes themselves or providing this information to other eMarketing companies or SPAMmers for the purpose of sending messages. The Privacy Act would typically also address prohibition of Address Harvesting and Dictionary Attacks. Needless to say, this Privacy requirement goes much beyond the need to address SPAM, and impacts a number of other aspects within the Kingdom.
2. Suitable conditions within their licensing agreements or specific industry driven initiatives to prevent stakeholder groups within the third stage of the SPAM Activity life cycle (Media), from using their infrastructure or allowing others to use their infrastructure, for the purpose of SPAMming. This also implies that they would ensure that they would immediately deactivate the account of any subscriber found to be involved in SPAMming activities. The industry driven initiative, such as a code of conduct, would apply to both stakeholders like the ISPs as well as eMarketing companies like the Bulk SMS service providers who need to comply with Opt-in or Opt-out requirements. This requirement for the Code of Conduct again goes well beyond the need to address SPAM, and could impact a number of other operational areas of these stakeholders as well.
3. An Anti-SPAM framework, that defines SPAM and provides provisions for penalties that would be enforced in the case of violations detected in this regard. An Anti-SPAM framework should also identify a mechanism to handle complaints, prosecutions and investigations.



4. It is possible that the principles of the Anti-SPAM framework, may be contained in full or partially, in domain specific legislations related to Banking, IT, and/or Telecom, and accordingly the Banking Act, e-Crime Law, e-Transactions Act, and the Telecom Act may also be relevant in this regard, though this is to be confirmed

The figure below depicts the logic used to identify the key legal domains and the relevant regulatory bodies/stakeholders that are potentially of direct relevance in the context of the review of the relevant legislations and enforcement.

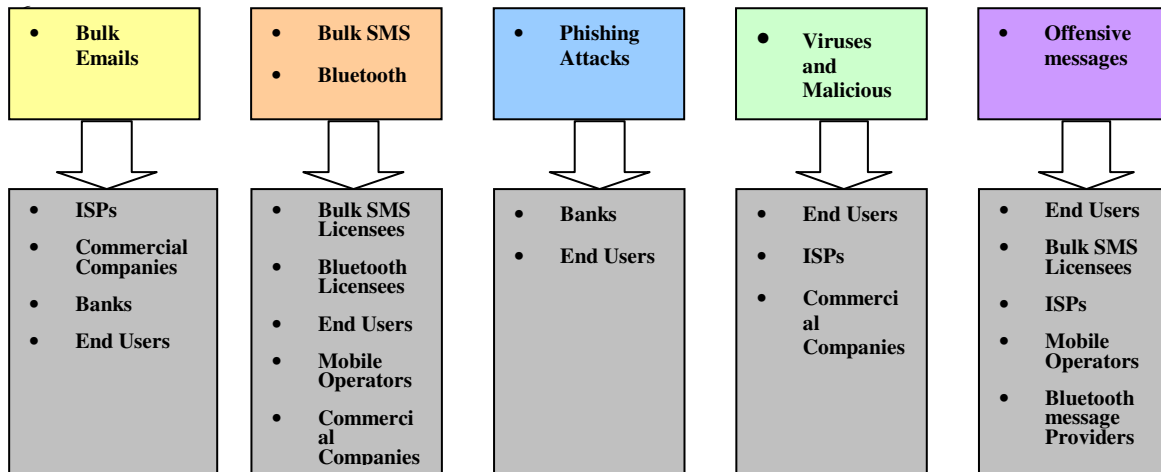


3.1 RELEVANT LEGAL DOMAINS

Using the above analysis, we concluded that the five most relevant legal domains that are of direct relevance in the review of existing legislations are:

1. The Privacy/Data Protection domain.
2. The Telecom domain, specifically in the context of the Telecom Act, and the licensing requirements of the various service providers.
3. The Banking domain, specifically in the context of the Banking Act.
4. The Anti-Commercial Fraud Law.⁴
5. The IT domain, specifically in the context of the e-Transactions Act and the e-Crimes Law.

⁴ Please refer to <http://www.commerce.gov.sa/> for further details regarding this law.



Accordingly, the key stakeholders that are considered to be of direct relevance in the context of the review of existing legislations and regulations that might have some anti-SPAM related considerations are:

1. The Ministry of Interior, due to their responsibility for Privacy, and their role in the enforcement of the various legislations in the Kingdom
2. The Communication and Information Technology Commission, in the context of their responsibility for the Telecom Act, the e-Crime Law and e-Transactions Acts, and the licensing of ISPs and bulk SMS service providers
3. The Ministry of Commerce (MOC) in the context of consumer protection regulations
4. SAMA in the context of its role in addressing requirements related to the Banking Act



4 ASSESSMENT OF THE RELEVANT LEGISLATIONS IN THE KINGDOM

The focus of this section is to provide a summary of the laws and regulations in the Kingdom considered relevant to this study. Given that there is no formal Privacy Law in the Kingdom, this section summarizes the intent, scope, and relevance of the laws related to:

- The Telecom Act and its Bylaws
- The Licensing Agreements with Bulk SMS Service Providers, Bluetooth providers and ISPs
- Conditions and Criteria for using Bluetooth Technology
- The Banking Laws and Regulations
- The Anti e-Crime Act
- The eTransactions Law

4.1 THE TELECOM ACT AND ITS BYLAWS

4.1.1 THE TELECOM ACT

Issued under the Council of Ministers resolution No. (74) dated 05/03/1422H (corresponding to 27/05/2001) and approved pursuant to the Royal Decree No. (M/12) dated 12/03/1422H (corresponding to 03/06/2001), the Telecom Act is the main regulatory framework for the Telecommunications Sector in the Kingdom of Saudi Arabia.

The Telecom Act stipulates the manner in which the Commission would regulate aspects related to:

- Frequency Spectrum
- Numbering
- Licensing
- Competition Rules
- Interconnection
- Equipment and Facilities
- Use of properties
- Violations and Penalties

The Telecom Act lists the type of actions by any operator, individual or a juridical person that would constitute a violation, and states that the penalty for such actions would be a maximum of SR 5 million. It also states that the penalties shall be proportionate to the violation committed and to the gravity of the violation in each individual case and will be imposed by a committee formed by a decision of the Board based on the nomination of the Commission Governor. The Commission's decisions can be appealed to the Minister. If the Commission's decision is upheld by the Minister, the concerned party has the right to appeal to the Grievance Dewan according to its Act.

While the Telecom Act does not explicitly mention SPAM, it stipulates that any usage of telecom media by a Telecom licensee to threaten or cause annoyance to the users is a breach of the Telecom Act, and can cause the licensee to bear legal consequences. Clause 11 from Article 37 in the Telecom Act, also states that "Misuse of telecommunications services, such as causing damage to the public



telecommunications networks or intentionally placing a message of an indecent or menacing nature or which causes panic or disturbance” by any operator, individual, or a juridical person constitutes a violation.

4.1.2 TELECOM BYLAWS

The Telecom Bylaws specify the procedures for executing the regulations in the Telecom Act. The Bylaws are presented in 15 Chapters addressing different aspects of the Telecom Act. These include:

- Chapter 1 : General provisions
- Chapter 2: Telecommunications Licenses
- Chapter 3 : Access to property
- Chapter 4 : Competition between service providers
- Chapter 5 : Interconnection
- Chapter 6 : Disputes between Service Providers
- Chapter 7 : Tariffs
- Chapter 8 : Relations Between Service Providers And Users
- Chapter 9 : Universal Access and Universal Service policies
- Chapter10 : Frequency spectrum
- Chapter 11: Numbering
- Chapter 12 : Telecommunications Equipment
- Chapter 13 : Protection and Prevention against intrusion
- Chapter 14 : Violations
- Chapter 15 : Closing Provisions

Articles 56, 57, 58 and 59 within Chapter 8 (Relationship between Service Providers and Users) of the Telecom Bylaws address the confidentiality of user information (Art-56), the confidentiality of user communication (Art-57), protection of user information (Art-58) and user complaints (Art-59). The provisions in these Articles are as follows:

- **Article 56 Confidentiality of User Information**

56.1 A service provider shall not disclose information other than the user’s name, address and listed telephone number to anyone without the user’s written consent or unless disclosure is required or permitted by the Commission or by law to another legally authorized public authority.

56.2 A service provider's liability for disclosure of user information contrary to this Article shall be determined in accordance with Chapter 13 of this Bylaw.

56.3 Upon request, users are permitted to inspect any service provider’s records regarding their service. Users shall have the right to require that any user information contained in their records that they can demonstrate is incorrect, be corrected or removed.

56.4 All user-specific information, and in particular billing-related information, shall be retained by a service provider only for billing purposes and retained only for so long as it is required by the laws of the Kingdom.



56.5 Nothing in this Bylaw shall be interpreted to prohibit or infringe upon the rights of concerned government agencies to exercise their rights to access otherwise confidential information relating to a user. Such access shall be made in accordance with the laws of the Kingdom.



• **Article 57 Confidentiality of User Communications**

57.1 Service providers shall take all reasonable steps to ensure the confidentiality of user communications in accordance with Article Nine of the Act.

57.2 Service providers shall not alter or modify a user communication.

57.3 For the purposes of tracing and locating a source of harassing, offensive or illegal calls;

- a. A user may request that the Commission authorize a service provider to monitor calls to the user's telephone;
- b. The Commission or other duly authorized authority in the Kingdom may direct a service provider to monitor calls to and from a user's telephone and the service provider shall comply with any such direction
- c. The service provider shall provide the Commission the information resulting from its monitoring of the user's telephone, including the telephone numbers that are the source of the harassing, offensive, or illegal calls and the dates of occurrence of such calls and their frequency; and
- d. The Commission may undertake any appropriate action to protect the public from harassing, offensive or illegal calls in accordance with the Commission statutes, and if necessary refer the matter to the appropriate authorities for further action

• **Article 58 Protection of Personal Information**

58.1 A service provider shall be responsible for user information and user communications in its custody or control and in that of its agents.

58.2 A service provider shall operate its telecommunications facilities and telecommunications network with due regard for the privacy of its users. Except as permitted or required by law, or with the consent of the person to whom the personal information relates, a service provider shall not collect, use, maintain or disclose user information or user communications for any purpose.

58.3 The purposes for which user information is collected by a service provider shall be identified at or before collection, and a service provider shall not, subject to this Article, collect, use, maintain or disclose user information for undisclosed purposes.

58.4 Service providers shall ensure that users' information is accurate, complete and up to date for the purposes for which it is to be used and that user information and user communications are protected by security safeguards that are appropriate to their sensitivity.

• **Article 59 User Complaints**

59.1 Service providers shall establish a separate division to receive complaints of users other than service providers. Service provider shall endeavor to eliminate the causes of complaints that are related to the quality or the method of providing the service and billing problems.

59.2 Service providers shall establish procedures to deal with complaints of users other than service providers. The procedures and any amendments thereto, shall be subject to the Commission's approval. The procedures shall be published in a suitable manner that is approved by the Commission.

59.3 Where there is a dispute between a service provider and a user that the parties cannot resolve amicably, the user may file a complaint with the Commission for resolution.

59.4 Complaints under this Article must request resolution of all outstanding issues in dispute.

59.5 Complaints shall be in writing and shall set out the facts and the relief requested. The user shall not be required to provide a copy of the complaint to the service provider.



59.6 The Commission shall render its decision as to whether the complaint is justified or not within ten (10) days of the filing of the complaint. The Commission may dismiss a complaint promptly if it determines that the complaint is frivolous or vexatious.

59.7 If the Commission considers that the appeal warrants investigation, it shall deliver a copy to the service provider. The service provider shall deliver a response within five (5) days or such longer period of time as the Commission may specify.

59.8 The Commission shall deliver the response of the service provider to the user. The user shall answer the service provider's response in writing within five (5) days or such additional amount of time as the Commission may allow.

59.9 The Commission may deal with the complaint on the basis of the written materials before it, or may require further information from one or both of the parties. The Commission shall issue a decision within thirty (30) days of the receipt of the response from the user, or notify the parties within that time that it requires additional time to issue its decision.

59.10 Service providers shall not disconnect or otherwise change any of the services then being provided to a user during the time for which they are the subject of a complaint by that user, without a decision from the Commission.

59.11 The Commission, if it deems that, according to Article Thirty Eight of the Act, a violation has occurred, may refer the matter to the violations committee.

The Telecom Act provides a broad framework to control the key telecom service providers, including the ISPs and the Content Providers (e.g. Bulk SMS service providers). The Telecom Act establishes the CITC as the nodal agency on all communication related matters. The licensing agreements defined for the ISPs and the Bulk SMS service providers are driven from the Telecom Act.

4.1.3 LICENSING AGREEMENTS

All parties wanting to provide information and communication technology services must obtain a license from the CITC. In this connection, CITC has issued a number of guidelines for those who have the desire to obtain the type (B) class license⁵, Bluetooth providers, Internet Service Providers and Bulk SMS Service Providers also need to obtain a Type (B) class license and are bound by the terms and conditions stipulated in the license. It is in this connection that we considered it pertinent to review the terms and conditions of these licenses also, for its relevance in addressing SPAM.

The Bluetooth message providers wishing to send offers and promote advertisements must obtain a license from CITC beforehand. This license addresses the privacy of the Bluetooth display name and

⁵ The Commission may issue two types of telecommunications licenses pursuant to Commission statutes: individual licenses and class licenses. There shall initially be two types of class licenses, Type A and Type B class licenses. The following services and networks shall, unless the Commission decides otherwise, require a Type B class license:

- a) Internet service provider (ISP) services;
- b) value-added network services;
- c) GMPCS or global mobile personal communication services;
- d) Public Call Office (PCO); and
- e) any other service or network that the Commission decides require a Type B class license



prohibits the sending of Bluetooth messages to persons not interested to receive these messages. Moreover, the Bluetooth provider shall keep the records of the sent messages for at a period of 6 months at least and ensure that their sent messages are free of viruses harmful to users' equipment and do not contradict with the Shari 'a laws, morals, ethics, general rules or conventions and not to include any violation to the prevailing regulations and Bylaws in the Kingdom.

The ISP Licensing Agreement applies to a range of internet based services apart from ISP, dialup, and broadband internet access, and also includes Internet Content Publishing and Internet Advertising.

The ISP Licensing Agreement states that among other conditions the licensee is obliged to:

- Not provide its services or Worldwide Web connectivity except through the methods determined by the CITC.
- Perform and observe all controls and instruction issued by the CITC and the other concerned governmental authorities.
- Maintain the confidentiality and accounts of the subscribers.

4.1.4 GAP ANALYSIS

The various articles in Telecom Act and its Bylaws as well as the Licensing Agreements, provide a reasonably sound basis for some of the key principles used in controlling SPAM, especially in terms of obliging Telecom Service Providers to keep user information confidential, protecting personal information, and addressing user complaints.

Some of the specific aspects related to obtaining consent prior to sending SMSes as well as specific controls on the ISP operations have been provided in the licensing agreements. Violations of the Telecom Act, its Bylaws, or Licensing Agreements, are punishable by penalties of up to SR 5 million.

However, these measures are not considered adequate to control SPAM.

In this context it is worthwhile to consider the codes of practice and best current practice guidelines prescribed by the ISP Associations in the UK and Australia. Examples of some of the practices recommended by them for the ISPs, in order to control SPAM more effectively, include:

- ISPs should ensure that their email systems will not relay email for unauthorized third parties.
- ISPs should ensure that all email generated within their own networks can be attributed to a particular customer or system, and should ensure that the immediate source of email which arrives from other networks can be determined.
- ISPs should operate appropriate arrangements for the handling of reports of abuse by their customers. They should publish contact details for their abuse team on their website, and also ensure that IP allocation entries in regional registries such as RIPE contain appropriate abuse team email addresses.
- Where abuse is proved, the ISP should take effective action to prevent the customer from continuing that abuse. The legal basis on which services are provided to customers should allow such action to be taken.
- ISPs should treat use of Unsolicited Bulk Email (UBE) to promote secondary services as an abuse of the provision of that secondary service.
- ISPs should not permit customers to distribute tools, or lists of email addresses, whose purpose is the sending of UBE.
- ISPs should disseminate information on the action taken in regard to customers who have sent UBE.



- ISPs should educate their customers on the nature of UBE, and should ensure that their customers have been made aware that sending UBE will be treated as unacceptable behavior.
- ISPs should inform their customers about any automated anti-SPAM mechanisms in operation and should educate their customers about any potential harmful side-effects.
- ISPs should also provide advice to their consumers detailing how they can protect themselves.

MAAWG (Message Anti-Abuse Working Group) also recommends inclusion of terms that state:

- Within the boundaries of the appropriate legal framework, ISPs and network operators must address the problem of compromised end-user equipment by establishing timely processes to allow such end-user equipment and network elements to be managed and eliminated as sources of SPAM;
- ISPs and network operators utilize industry standard technology to authenticate their email and/or their sources;
- ISPs and network operators should block potentially infecting email file attachments. In the case of filtering email or email file attachments based on content properties, in the context of any required legislation prior agreement is to be attained from the customer;
- ISPs and network operators actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and respond appropriately;
- ISPs and network operators establish appropriate inter-company processes for reacting to other network operators' incident reports, also accepting end user complaints.
- ISPs, network operators and enterprise email providers should communicate their security policies and procedures to their subscribers;
- ISPs and network operators attempt to send non-delivery notices (NDNs) only for messages originated by their own account holders;
- ISPs and network operators take measures to ensure that only their account holders use their e-mail submit servers;
- ISPs and network operators ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information, and that this information includes points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address;
- ISPs and network operators ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date forward and reverse DNS records and WHOIS and SWIP entries;
- that all local area network (LAN) operators are compliant with Request for Comments (RFCs) 1918 — "Address Allocation for Private Internets," and that in particular, LANs do not use IP space globally registered to someone else, or IP space not registered to anyone, as private IP space.

Inclusion of such conditions in the Telecom Act, its Bylaws, licensing agreements, or in a separate SPAM related ISP Code of Conduct that the ISPs need to abide by, will enable better control on the initiation and spread of SPAM through media like the ISPs.



It should be noted that while CITC has a strong regulatory framework in place in most cases, the lack of periodic audits, has resulted in weaknesses in the implementation of the frameworks. This also applies to the ISPs licensing agreements.

4.1.5 CONTROLLING E-MARKETING SERVICE PROVIDERS

In order to address SPAM effectively, it is imperative that suitable control be imposed on the activities of eMarketing Service providers, including Bluetooth messages providers and Bulk SMS service providers, through regulatory guidelines and other means.

The “Special Terms and Conditions of Type (B) Class License for Bulk SMS Service” addresses the licensing conditions for the Bulk SMS service providers. Key conditions included in these Terms and Conditions include:

- No message shall be sent to the subscriber without his approval
- All ads and/or promotional materials for the service shall contain numbers allocated only for the service advertised. Also, the cost of the message shall be written clearly and shown in the video ads, so that the beneficiaries can have adequate information before obtaining the services.
- Any message shall be sent through licensed message centers and telecommunication networks in the Kingdom.
- Coordination shall be made with licensed telecommunication network operators within the Kingdom to use their networks within the Kingdom in sending the bulk short messages to subscribers outside the Kingdom.
- Licensee shall be responsible for any legal or financial consequences that may be incurred by the operator, if the Licensee breaches the international agreements governing the relation between the internal operators and the operators outside the Kingdom, such as **GSM Association AA.19** agreement for messaging between international operators.
- If the service provider is to use the Internet in sending and receiving the messages, all servers shall be based in the Kingdom.
- The service shall not be used as a means for the collection of amounts due for other services, such as the Internet subscription fees, without prior permission from the CITC.

These conditions do impose significant constraints on the Bulk SMS Service Provider’s ability to send SPAM messages, provided its implementation is suitably monitored through periodic audits.

However it should be noted that key gaps that exist relate to controls on:

- The process used for obtaining user consent
- The process used for maintaining user consent records
- Inclusion of accurate information about senders/message authorizers
- Provision and operation of a functional unsubscribe facility
- Sending commercial electronic messages about age sensitive material; and
- Complaints handling.

It is useful to consider practices used in other countries in this regard, particularly the eMarketing Code of Practice in Australia, which provides a set of guidelines that all eMarketing (content providers) in Australia need to abide by. The *Telecommunications Act 1997* provides the Australian

Final Version	Page 18 of 64 Confidential - Internal Use Only	
----------------------	---	--



Communications Authority with powers to investigate complaints, issue warnings to comply and direct compliance with registered codes of practice (whether the industry member is a signatory to the Code or not). A failure to comply with a direction issued by the ACA can result in court action and the imposition of pecuniary penalties. These guidelines include recommendations that state:

- Message Originators must ensure they do not send, cause to be sent or authorize the sending of Unsolicited Commercial Communications.
- Message Service Providers must ensure that they do not send or cause Unsolicited Commercial Communications to be sent.
- Message Originators and Message Service Providers may send, authorize the sending or cause the sending of Commercial Communications to Recipients or Relevant Electronic Account Authorities providing that:
 - The Recipient has provided Express Consent to receive such Commercial Communications
 - It can be reasonably Inferred through conduct of the Recipient that the Recipient has Consented to receive such Commercial Communications (Inferred Consent)
 - The process that Message Originators and Message Service Providers employ to gain Consent from the Recipient or Relevant Electronic Account Authority must be clear and transparent
 - Where at any time a Recipient or Relevant Electronic Account Authority has expressly notified the Message Authorizer, Message Originator or Message Service Provider that Consent is withdrawn or denied, the Message Originator or Message Service Provider must not rely on circumstances which might otherwise be considered Inferred Consent to send a Commercial Communication
 - Where a Complaint has been lodged with the ACA or a Recognized Industry Body, the onus is on Message Originators to demonstrate with sufficient evidence that Consent has been obtained
 - Message Originators must only send or cause to be sent Commercial Communications to Third Party Contacts, including Recipients listed on a swapped, rented or purchased list, where all reasonable steps have been taken to confirm that the Data Provider has obtained Express or Inferred Consent from the Recipient or Relevant Electronic Account Authority to disclose their details to a third party Message Originator or Message Service Provider
 - Message Originators and Message Service Providers must provide sufficient information to the Recipient or Relevant Electronic Account Authority so that they know that their details will be disclosed and used by a third party Message Service Provider
 - Message Originators and Message Service Providers must take all reasonable steps to ensure Recipients or Relevant Electronic Account Authorities do not receive MWT Commercial Communications between the hours of 9pm and 8am Monday to Friday and 9pm to 9am on weekends, unless the Recipient or Relevant Electronic Account Authority has expressly invited delivery within these hours or been notified in advance that this will be the case
 - Message Originators and Message Service Providers must ensure that Commercial Communications that include a Forwarding Facility contain a clear recommendation that the Recipient should only forward the Commercial Communication to persons with whom they have a relationship, where that relationship means that person could be said to have Consented to receiving Commercial Communications
 - Message Originators and Message Service Providers must ensure that any Commercial Communications they send contain information identifying the Message Originator or Message



Authorizer in such a way that they can be easily recognized and contacted by the Recipient. The information must remain valid for 30 days after the Commercial Communication is sent.

- Message Originators and Message Service Providers must ensure that the Contact Mechanism is provided at low cost and is easy for the Recipient or Relevant Electronic Account Authority to use.
- Express Consent of the Recipient or Relevant Electronic Account Authority must be obtained by the Message Originator before supplying Paid Subscription Services.
- For each Commercial Communication, Message Originators and Message Service Providers must provide an easy-to-use, Functional Unsubscribe Facility allows the Recipient or Relevant Electronic Account Authority to opt-out of receiving further Commercial Communications sent from the Message Originator or authorized by the Message Authorizer by, at least, the same Device by which they were contacted;
- Message Originators and Message Service Providers must clearly state to which products or services the Functional Unsubscribe Facility relates.
- Where the content of a Commercial Communications seeks to promote or inspire interaction with a product, service or event that is age sensitive, the Message Originator must take reasonable steps to ensure that such content is sent to Recipients who are legally entitled to use or participate in the product service or event
- Message Originators and Message Service Providers must have in place a Complaint handling system (i.e. internal procedure for dealing with Complaints) which is fair, effective, confidential and easy to use by the complainant
- Message Originators and Message Service Providers must ensure that the Contact Mechanisms by which a complainant can lodge a Complaint are not charged at a rate that exceeds the standard rate for that Contact Mechanism

As is evident from the above recommendations, there are significant gaps in the obligations imposed on eMarketing companies by the relevant licensing agreement and laws. Unless these gaps are addressed suitably, either through incorporation of these clauses in the licensing agreement or through a suitable eMarketing Code of Conduct, there are significant limitations on the extent of control that can be imposed on the eMarketing companies.

It is also imperative that in conjunction with the tightening of controls of the licensing terms and conditions, that a suitable audit mechanism is also implemented that verifies the manner in which the proposed conditions are being implemented by the Content Providers.

4.2 THE MONETARY AND BANKING LAWS AND REGULATIONS

The Monetary and Banking Laws and Regulations provides the charter for the Saudi Arabian Monetary Agency, which is focused on meeting the objectives of issuing and strengthening the Saudi currency and to stabilize its internal and external value, dealing with the banking affairs of the Government, and regulating commercial banks and exchange dealers.

The Banking Control Law provides the regulatory framework for banking operations in the Kingdom. It addresses the licensing requirements for Banks to operate in Saudi Arabia, requirements related to deposit liabilities and statutory deposits, limits related to provision of loans and guarantees, scope of operations, audit and reporting requirements, as well as suitable penal provisions for contravention of any of the articles in the Law. Other related laws deal with currency, forgery, and money laundering.

Final Version	<p>Page 20 of 64</p> <p>Confidential - Internal Use Only</p>	
---------------	--	--



While SAMA does provide Internet Banking Security guidelines, there are no explicit instructions published as yet on the manner in which Phishing related issues need to be addressed by the Banks, both in terms of user education and awareness, as well as reporting Phishing cases.

SAMA indicated that it has suggested that Banks implement suitable controls so that even if a Phishing attack were successful in obtaining a user account's username and password, it would not be possible to transfer the money in the account to another account easily. Since creation of a new beneficiary takes 24-48 hours in most cases, it significantly limits the ability to transfer funds immediately, limiting the impact of a Phishing attack.

Based on discussions with SAMA officials, we were informed that a formal procedure for reporting Phishing complaints is being developed currently in conjunction with the Banks as are user education and awareness guidelines.

It was considered that Phishing attacks, particularly if it has not resulted in a financial crime, would be addressed by the newly promulgated Anti e-Crime Act, though it was considered imperative to strengthen the Anti e-Crime Act enforcement mechanism, without which the effectiveness the Law could be limited.

In this connection, it is useful to consider that Article 4 of the Anti e-Crime Act stipulates that

“ . . any person who commits any of the following crimes shall be punished by imprisonment for 3 years maximum and a fine of no more than SR 2 million, or either one of them.

1. Take possession for himself or for a third party, through an information network, a computer, or a similar means, of cash money or a voucher or signing such a voucher utilizing a fraudulent means or a fake identity or impersonation if such an action is meant to deceive the victim.
2. Use the Information network, a computer, or similar means to access unlawfully and unrightfully bank accounts, credit card information or the like, or to utilize such information to obtain personal data, funds or services “

According to the existing situation, there is no well defined and documented process in place for handling complaints.

Phishing attacks are typically reported by Banks to SAMA initially, who then report it directly to CITC, who is responsible for shutting down access to the phishing site. In some instances, banks report directly to CITC. All other requests (non-phishing) to block Web sites go first to “National Security Committee” headed by MoI which notifies CITC to shutdown the reported Web site address. CITC blocks phishing web sites within a short period of time and informs all DSPs to update their systems accordingly. The time needed to block the reported Web sites by DSPs might take up to 24 hours in some cases.

However, the new Filtering Management System (FMS)⁶ which is still currently under the development phase can be customized to accommodate SPAM-related complaints..

SAMA generally refers all cases of SPAM and/or Phishing attacks to the Ministry of Interior. It also recognizes the role of CITC in assisting MoI in investigating such crimes.

⁶ The FMS will be a complete system to manage and automate all the tasks related to filtering. This system should automate the reporting process, generate statistical reports, and provide a tool to enforce the filtering requirements.



It was considered imperative that in order to enhance the overall effectiveness of the enforcement mechanism, a formal coordination mechanism be established quickly between MoI and CITC, and that trained IT Crime investigation specialists be used in investigating such cases.

4.3 ANTI-COMMERCIAL FRAUD LAW

According to the commercial regulations in the Kingdom, the royal decree number 45, dated 14/8/1381, every merchant must conduct his trading activities with due diligence away from deeds that involve any kind of scamming, misleading, or cheating of the consumer.

The Anti-Commercial Fraud Law provides the Ministry of Commerce (MOC) with the main responsibility of dealing with all forms of consumer-related commercial fraud. Moreover, the enforcement of this Law, i.e., the detection and investigations of violations of the Anti-Commercial Fraud Law and its Bylaws is mainly the responsibility of MOC. Moreover, the Anti-Commercial Fraud Law assigns the MOMRA the task of monitoring the expiration dates of foods in the market. As per the regulations of the Law, six commissions were set up scattered over different areas in the Kingdom. A nodal commission, called the National Commission for Consumer Protection, takes the lead and is responsible for leading the various commissions, planning and monitoring the execution, and running consumer protection awareness programs.

In regard to this law, pecuniary penalties, shutting down the business, imprisonment, and compensation can be applied to every one who aids, abets or directly commits scamming, misleading, fraud, tricking or cheating consumers regarding:

- The description or advertisement of an item, i.e. misrepresenting the item and misleading or tricking the consumer
- The item's nature, components, types or main features
- Item's origin
- Item's value, its weight, size, price, etc

It was considered that in order to deal with violations regarding the content of the message, in particular, fraudulent and misleading advertisements, the Anti-Commercial Fraud Law will be the suitable reference to decide if the content of the message is illegal and consequently taking the actions based on the sanctions provided by the law.

4.4 ELECTRONIC TRANSACTIONS ACT

The objectives of the Electronic Transactions Act are to:

1. Set unified regulatory standards to streamline use of electronic transactions and signatures.
2. Enhance confidence in the soundness and validity of electronic transactions, signatures and records.
3. Facilitate usage of electronic transactions locally and internationally in fields such as e-government, trading, medicine, education and e-payments.
4. Eliminate barriers in using electronic transactions and signatures.
5. Prevent misuse of electronic transactions and signatures and related fraud.

Given the nature of the law, there are limited provisions in the law that are focused on controlling aspects related to SPAM, though there are suitable provisions against specific types of fraud. For instance, the eTransactions Act provides protection against impersonation of another person's identity,



forgery of electronic signatures or digital certificates etc as well as unauthorized access into systems for the purpose of misusing such certificates.

4.5 ANTI E-CRIME ACT

The Anti e-Crime Act aims at creating legal and regulatory standards to combat information, computer and internet crimes through specifying /determining the relevant crimes and punitive actions for each crime or violation, in order to achieve the following:

1. Maintain information security.
2. Safeguard the rights associated with legitimate use of computers and networks.
3. Safeguard public interests, morals, and communal values.
4. Develop and safeguard the National Economy

While the Anti e-Crime Act does not specifically or fully address SPAM, it does address certain aspects of SPAM, including aspects relating to using SPAM for Phishing purposes, spreading viruses, or publishing content that could be considered detrimental to the Kingdom's economy or security, offensive to its religious values and morals, or contrary to the privacy of resident individuals.

Article 3 provides for suitable punishment for Phishing related crimes and states that “. . . any person who commits any of the following crimes shall be punished by imprisonment for 3 years maximum and a fine of no more than SR 2 million, or either one of them.

1. Take hold for himself or for a third party, through an information network, a computer, or a similar means, of cash money or a voucher or signing such a voucher utilizing a fraudulent way or a fake identity or impersonation if such an action to deceive the victim.
2. Use the Information network, a computer, or similar means to access unlawfully and unrightfully to bank accounts, or a credit card information or alike, to utilize such information to obtain personal data, funds or services

Article 5 of the Anti e-Crime Act stipulates that any person who commits any of the following crimes shall be punished by imprisonment for maximum of 4 years and a fine of maximum SR 3 million or either one of them:

- Unauthorized access of a site or information system, with the intention of deleting, destroying, divulging, damaging, altering or re-publishing personal information
- Access through an information network or a computer or through any similar means such as applications, software, etc, which may disrupt or interrupt the work of the information network, or destroy, delete, erase, disclose, damage or alter software or data used by or stored in the network
- Interrupt, disrupt, or interfere, deliberately and unrightfully, by any means through the information network, a computer or any similar means, access to services, hardware, software or information sources

Article 6 of the Anti e-Crime Act stipulates that it is a crime to “Develop material and data related to pornography or gambling, which contradicts the general values, or publish or promote such materials”

Article 7 of the Anti e-Crime Act stipulates that it is a crime to “Access deliberately and unlawfully to any site or system, directly or through an information network, a computer or similar means to obtain data that harm the country's internal or external security or national economy. If access is for deleting such data or information, damage or destroy such data, or transmit harmful ideas or thought, the minimum limit of punishment will be imprisonment for 3 years.

<p>Final Version</p>	<p style="text-align: center;">Page 23 of 64 Confidential - Internal Use Only</p>	
-----------------------------	---	--



Thus while we believe that the Anti e-Crime Act establishes a suitable basis for prosecution of SPAMMers involved in publishing pornography, content considered offensive to the Kingdom's economy or security as well as content considered inappropriate to the religious and moral values, and also the use of SPAM for Phishing or spreading harmful viruses and other malware, it does not address:

- The definition of SPAM, including the requirement for the user's consent to receive such messages
- The prosecution of SPAMMers involved in sending unsolicited commercial advertisements, on the assumption that the user's consent is a requirement for sending such commercial messages and advertisements
- The minimum requirements that messages containing commercial advertisements need to comply with, including the need to include a provision for unsubscribing from such messages

It should also be noted that the Anti e-Crimes Act is focused on the prosecution of personnel and entities involved in such activities, operating from Saudi Arabia. Accordingly, as with other such laws, the Anti e-Crime Act is unlikely to be able to address the SPAM that might have originated in another country.

4.6 CONCLUSION

Having reviewed laws in the Kingdom considered to be relevant in the context of addressing SPAM and its effects, it was concluded that:

- There is no Privacy Law in the Kingdom to control the misuse of eMails and mobile numbers, obtained for specific purposes by organizations in Kingdom, for the purpose of SPAMming. It is proposed that the newly established unit within the General Security forces specialized in fighting eCrimes should be addressing the issue of trading and exchanging contact details in black markets as part of its duties.
- While the existing Telecom Law, and its Bylaws, provide a good basis for the control of telecommunication service providers in the Kingdom, neither it nor its Bylaws address SPAM fully. While licensing agreements exist with ISPs and Bulk SMS Service Providers, there are significant gaps in the terms and conditions in the context of its ability to address SPAM fully
- The Electronic Transaction Law was not considered directly relevant to the SPAM issue
- While the Anti e-Crimes Act does deal with certain aspects of SPAM, particularly in relation to sending of offensive messages from a content perspective, spreading viruses, and Phishing, it falls short of addressing the SPAM issue fully in that it:
 - Does not explicitly define and deal with SPAM
 - Does not explicitly deal with specific forms of SPAM, such as fax SPAM
 - Does not explicitly indicate if explicit, implicit, or inferred consent of the receiver is a requirement, for sending commercial advertisement messages
 - Does not stipulate if unsolicited commercial messages can be considered SPAM
 - Does not state the minimum requirements for legitimate commercial messages, such as the unsubscribe option for users to request the sender not to send such SPAM anymore



- Does not specify the penalties for sending or causing to send unsolicited commercial messages, if this was to be considered SPAM
- In order to illustrate this gap further, we have considered the key requirements, specified by OECD, to comprehensively deal with SPAM in a regulatory framework. These include specific consideration of:

- **Technical Elements**

While controls on eMarketing through SMSes have been partially addressed in the General and Specific Terms and Conditions of Type (B) Class License for Bulk SMS Service, no such controls have been imposed on eMarketing (sending of commercial messages) through eMails or faxes. Clause 11- Section 37 of the Telecom Acts prohibits the “Misuse of Telecom service to cause annoyance” but does not explicitly define what could be considered annoyance.

- **Consent**

In its Anti-SPAM Regulation document published in November 2005, OECD’s Task Force on SPAM introduced “consent” as a fundamental consideration in developing anti-SPAM legislations. A number of conceptual frameworks have been utilized in relation to consent, including opt-in and opt-out models and provisions that allow for consent to be inferred where there is a pre-existing relationship.

While the General and Specific Terms and Conditions of Type (B) Class License for Bulk SMS Service explicitly specify that consent of the receiver is required before sending commercial messages to them, no such stipulations have been made in any of the existing legislations in the context of eMarketing through eMails, faxes, or other means.

- **Privacy**

According to OECD’s Task Force on SPAM, the term privacy is generally linked to that of use of personal data. Depending on the jurisdiction, personal data may be considered to include information such as addresses (e-mail and otherwise), personal preferences, and data such as age/medical conditions of individual natural persons.

While no Privacy Act has been legislated in the Kingdom, various aspects of Privacy have been dealt with separately in various legislations. For instance:

- Article 40 of the Basic Law of Governance in the Kingdom of Saudi Arabia states that correspondence by telegraph and mail, telephone conversations, and other means of communication shall be protected. They may not be seized, delayed, viewed, or listened to except in cases set forth in the Law.
- Article 6 of the newly enacted Anti e-Crime Act in the Kingdom provides for up to five years in prison and a fine of up to 3 million riyals for breaching personal privacy by illegally “sending” private information about individuals using data networks.
- The Telecom Bylaw in its clause 1 of article 56: Confidentiality of User Information prohibits *telecom service providers* from disclosing users’ information except the user’s name, address and listed phone number to anyone without the written consent of the user. This implies that all other information about the user stored by the service provider shall be kept private.

However, there is no law which explicitly prohibits the use of personal information such as addresses (e-mail and otherwise), personal preferences, and data such as age/medical conditions of individual natural persons, from being used for purposes other than the purpose for which it was collected by any organization in the Kingdom, including eMarketing service providers.



- **Commercial Elements**

The majority of SPAM is sent in order to achieve a profit – through the sale of goods or services, or through some sort of fraud. Arguably, one of the better ways of reducing SPAM is to reduce the economic benefits that the SPAMmer receives from sending SPAM messages. For this reason, many legislative definitions of SPAM stress the commercial nature of SPAM – that SPAM is sent for marketing purposes or to achieve financial gain.

Accordingly, it is important that eMarketing or sending of commercial messages through any electronic media should be suitably regulated. At this point, while the General and Special Terms and Conditions of Type (B) Class License for Bulk SMS Service providers do impose some restrictions, there are no such constraints imposed on eMarketing through other means, including eMails, Bluetooth, Instant Messaging (IM) and faxes.

- **Bulk**

In keeping with the OECD recommendations, some SPAM regulators specify a threshold, beyond which messages (e-mails, SMS or Fax) sent above this cut-off point are designated as SPAM. Other regulators, like the ACMA in Australia, do not make particular reference to bulk messaging, thereby allowing that even a single unsolicited commercial electronic message could be SPAM.

While Clause 11- Section 37 of the Telecom Acts prohibits the “Misuse of Telecom service to cause annoyance” it does not explicitly the threshold beyond which eMarketing messages could be considered an annoyance. Since SPAM mails have not been dealt with explicitly in any legislation, and no other qualification regarding the threshold, beyond which the sender could be considered to be sending SPAM messages, has been provided in any other legislation, it is not clear if this could be construed to imply that even a single unsolicited electronic message could be considered to be SPAM`.

- **Content**

According to OECD, one of the main concerns of the community and regulatory bodies is the illicit content of a considerable amount of SPAM - including those that promote pornography, illegal online gambling services, pyramid schemes, get-rich-quick schemes or misleading and deceptive business practices. The stateless nature of messages has led to it being used to convey commercial offers and other content of a dubious nature, often with the true origin of the message disguised. The indiscriminate method of distribution is of particular concern as it is common for minors to receive SPAM that is pornographic, illegal or offensive.

In the Kingdom of Saudi Arabia, content of the messages is of additional concern especially if it contradicts the religious and moral values of the Kingdom. Gambling, pornography, drugs and alcohol are strictly prohibited in the Kingdom.

While the Anti-Commercial fraud law deals with the content of the message if it is of fraudulent and misleading nature, the Anti e-Crime Act effectively deals with messages considered to be offensive to the Kingdom’s security or economy as well as religious or moral values. The Anti e-Crime Act also prohibits the sending of any kind of pornographic or obscene messages, or promotes gambling, alcohol, drugs or the methods to smuggle and utilize these substances.

- **Damage, Threat and Annoyance**

SPAM causes harm to a wide range of parties and systems. The costs to the victims of SPAM vary. From a systemic point of view, damage may be done by SPAM that effects a denial of service to parties, or by SPAM that is used as a vehicle for other malicious tools, for example, viruses. This systemic damage imposes costs in relation to infrastructure, human resources and in terms of opportunity cost when systems are damaged. Secondly, the cost of SPAM can be measured in terms of a focus on the content of the SPAM.

<p>Final Version</p>	<p style="text-align: center;">Page 26 of 64 Confidential - Internal Use Only</p>	
-----------------------------	---	--



While damage and threat are clearly addressed in article 3 of the Anti e-Crime Act, annoyance is not defined. Also section 37 of the Telecom act prohibit the use of technology to cause annoyance to others, however, the term Annoyance is not defined, and it remains ambiguous what is meant by annoyance.

The use of emails, SMS messages, and Fax to cause damage, threat or annoyance can now be prosecuted under Article 3 of the e-crime law. Annoyance is not defined or quantified, but can still be considered under invasion of privacy or causing damage to the others.

Also, other form of threat and damage like spreading viruses can be prosecuted under Article 5 of the Anti e-Crime Act that prohibits the use of the information systems and information networks to disrupt or interrupt the work of the information network, or destroy, delete, erase, disclose, damage or alter software or data used by or stored in the network.

- **Requirements for Legitimate Messaging**

Legitimate messages are sent through the same messaging media as SPAM. According to OECD recommendations, unless there is a desire to cease use of a messaging media, or prevent its use for commercial transactions, then any response to SPAM also needs to define what messaging is appropriate and lawful.

While the Special Terms and Conditions of Type (B) Class License for Bulk SMS Service impose the use of the sender's name, a clear price of the services promoted, and an option to unsubscribe from those messages, these conditions are only applicable to bulk SMS operating under a license from CITC. No such conditions exist for eMarketing through eMails, IM, Bluetooth, or faxes.

- **Exemptions and Restrictions**

Exemptions and restrictions are subject to the definition of SPAM. SPAM must be defined, and according to the definition of SPAM, some content could be exempted from anti-SPAM regulations, by example, messages containing religious content. Indeed, the solicitation of monetary contribution through bulk communications has been prohibited as per a recent directive.

While the existing legislations do address SPAM in certain aspects, it is evident that significant gaps still exist in the legislative framework within the Kingdom that still needs to be addressed.



5 REVIEW OF LEGAL CASES

The purpose of this review was to consider the manner in which selected recent SPAM related complaints and legal cases were dealt with, specifically from the perspective of analyzing the gaps in the current Anti-SPAM related legislations and regulations that might have hampered the prosecution of the offending parties.

5.1 APPROACH USED

The three cases provided by CITC, for the purpose of the review, involved different types of complaints. None of the three cases had been prosecuted in a court of justice and no penal action was taken against the perpetrators. We reviewed the cases to identify the gaps that prevented the indicated prosecution from reaching the specialized courts of justice.

Each of the three cases was addressed separately by considering:

- The nature of the case – presented as an executive summary of each case
- The approach taken to handle the case – This section looks at the various steps taken during the prosecution process (Investigations, Forensics, etc...)
- The action taken – This section describes the action taken by CITC against the alleged offender in each case.

The analysis of the cases focused on gaps in the existing legislations that hampered the prosecution.

5.2 CASE-1: EMAIL SPAM CASE BY MICROSOFT AGAINST SAHARA

Nature of the Case

Microsoft Saudi Arabia filed a complaint with CITC against Sahara Al-Jazeera, an ISP registered in the Kingdom of Saudi Arabia and licensed to provide Internet and Bulk SMS services in the Kingdom of Saudi Arabia by CITC. Microsoft claimed that their SPAM-trap mailboxes captured a number of SPAM emails sent by Sahara Al-Jazeera on behalf of Giant Stores in the Kingdom of Saudi Arabia.

The emails contained a link to the Giant Stores' (Saudi Arabia) website. The messages were sent by Sahara without the consent of Microsoft and involved use of a different domain owned by Sahara Al-Jazeera to send the SPAM messages. The eMails did not have a clear return eMail address nor an "unsubscribe" option.

Microsoft used an international forensics company to trace the originator of the email. The forensics investigation linked the eMail to Sahara Al-Jazeera, a locally registered ISP in the Kingdom of Saudi Arabia.

Microsoft then filed a complaint with CITC, through their lawyers in the Kingdom of Saudi Arabia, along with a copy of the forensic investigation report.

The Approach Taken

CITC undertook the investigation of the case. The evidence provided by Microsoft was considered in detail.

A representative from Sahara Al-Jazeera was called in by CITC for questioning. The representative admitted the company's responsibility for sending the emails, which was found to have been sent out in bulk to eMail addresses, obtained using an eMail harvesting software.

Final Version	Page 28 of 64 Confidential - Internal Use Only	
---------------	---	--



The investigation report, filed by CITC, stated that this case could only be prosecuted under Clause 11- Section 37 of the Telecom Act, by considering it a case of “Misuse of telecom to cause **annoyance**”. However, since the term “annoyances” had not been clearly defined in the Telecom Act and was considered to be ambiguous, it could not be applied to this case. This was particularly so since such eMails were sent out only 2-3 times a month.

The Action Taken

Since it was not possible to consider the complaint an offence under any of the existing legislations or regulations, CITC recommended that Sahara Al-Jazeera be made to sign a commitment paper confirming that they would refrain from sending similar messages in the future.

The CITC legal department send the report and the related recommendation to the Committee of Arbitration and Dispute Resolution in Telecom related matters. The Committee was requested to revert within a stated period in case they did not agree with the recommendation. Since the Committee did not revert with a contradicting decision within the stated notice period, the case was considered closed by the legal department.

Analysis

The messages sent by Sahara Al-Jazeera satisfy most of the conditions used most commonly to define SPAM mails, particularly:

- The mail was unsolicited: The complainant did not opt to receive mails of this nature from Sahara Al-Jazeera
- The mail did not have clear return eMail addresses: Sahara Al-Jazeera masked the real originating email address, and instead used another email address in the sender’s field
- The mail was commercial in nature: The emails sent were promotional in nature, and were aimed at making financial gain to the beneficiary (Giant Stores)
- The mails were sent out in bulk: Sahara Al-Jazeera’s representative admitted sending these commercial email to a large list of email addresses, even though these type of emails were sent out only once or twice every month
- The mails used harvested address lists either directly or using dictionary attacks: The Company’s representative admitted using “email hunter”, an email harvesting software, to compile the list of email addresses to which the commercial emails were sent
- The mails did not have an unsubscribe link: The mails did not have an opt-out link, as documented in the investigation report.

However, since there is no legal definition of SPAM in the Kingdom of Saudi Arabia, the emails sent by Sahara Al-Jazeera could not formally be classified as SPAM.

As identified by CITC, while Clause 11 – Section 37 of the Telecom act prohibits “Misuse of technology to cause annoyance”, the definition of “annoyance” is not clear and as such it was not clear if such emails could be considered to be an annoyance and if so, the threshold (number of emails) that would qualify as an annoyance.

With some exceptions, the laws in Saudi Arabia do not explicitly prohibit the sending of specific types of content in messages, be it commercial, financial, political, or other types of content. The exceptions relate to the use of electronic means to threaten or blackmail others.

While the need for consent of the users before sending commercial messages has been addressed for SMS messages in the SMS Service Providers’ Obligations within the Special Terms and Conditions of Type (B) Class License for Bulk SMS Service, none of the existing laws or regulations in the

<p>Final Version</p>	<p style="text-align: center;">Page 29 of 64 Confidential - Internal Use Only</p>	
-----------------------------	---	--



Kingdom insist on the need to obtain the consent of the users before sending commercial eMail or fax messages.

While protection of user information and non-disclosure of users' private information by telecom service providers to third parties is provided in Sections 56, 57, and 58 of the CITC bylaw and Article 10 of the Class B licensing conditions, there are no stipulations in any of the Telecom or other Laws that prohibit the use of eMail harvesting software to obtain eMail addresses for the purpose of eMarketing. Furthermore, while Clause 10 – Article 10 of Class B services licensing conditions prohibits the use of subscribers' telephone numbers for use in advertising campaigns, it does not prohibit use of other personal information, such as eMail addresses, to do so.

No law in the Kingdom currently stipulates that commercial messages sent by eMail, SMS, fax or other means should clearly include the senders address or an unsubscribe option.

The current laws contain penal codes for misuse of technology, breach of Telecom Act, breach of e-crime law, and breach of CITC bylaws and licensing conditions. These penalties could be in the form of fines, withdrawal of licenses or any other penalty decided by the Committee of Arbitration and Dispute Resolution within CITC. But since this case does not satisfy the conditions of misuse of technology, no penal action could be taken against Sahara Al-Jazeera.

5.3 CASE-2: MOBILE SPAM

Nature of the Case

The case was filed with CITC by a user with a complaint related to the receipt of unsolicited SMS messages on his mobile containing links to premium charge dating numbers outside the Kingdom of Saudi Arabia. The dating numbers connected callers to a live chat room, with various other users connected from within Saudi Arabia and other countries, to exchange obscene chats.

The complainant said that he was not able to opt-out of receiving such messages and asked the commission to intervene and prevent such messages from reaching his and other mobiles in the Kingdom, specifically because the SMS messages could be sent to mobiles owned by minors and that the disturbing and extremely obscene nature of the chat rooms was not suitable for minors and contradicted local and Islamic values of the Kingdom of Saudi Arabia.

The cost of calling the premium rate number had also not been indicated clearly by the advertiser.

Saudi Telecom did not respond to CITC's request to identify the sender of the message.

The Approach Taken

Since the message was sent from a place that was outside the jurisdiction of the laws of the Kingdom of Saudi Arabia, and did not contain a link to a premium rate number in Saudi Arabia, it was considered that the laws of Saudi Arabia could not be applied to either the initiator or the beneficiary of the revenue generated from sending similar messages.

The Action Taken

CITC did not file an investigation report in this case. No entity was prosecuted, and there was no involvement from lawyers or courts.

CITC consulted with both mobile operators in the Kingdom on what could be done to prevent such cases. The mobile operators indicated that while these types of messages could not be stopped completely, a few technical measures could be implemented to filter messages based on their content. Joining international treaties (e.g. AA.19 Agreements), in this regard, would also help limit the damage caused by similar messages.

<p>Final Version</p>	<p>Page 30 of 64 Confidential - Internal Use Only</p>	
-----------------------------	---	--



CITC requested Saudi Telecom to identify the source of similar messages and to take suitable action to block content of similar nature in the future. Saudi Telecom confirmed that they had taken suitable action to block all messages coming from that bulk SMS service provider in the future, and also were in the process of implementing certain technical measures to filter messages containing content considered obscene or going against the religious and social values of the Kingdom of Saudi Arabia. They did not respond with the identity of the sender.

Analysis

The SMS messages sent from outside the Kingdom again satisfy most of the conditions used most commonly to define SPAM mails, particularly since:

- The messages were unsolicited: The complainant did not opt to receive SMSes of this nature from the party sending such messages
- The messages were commercial in nature: The messages sent were promotional in nature, and were aimed at making financial gain to the beneficiary (the owner of the premium rate number)
- The messages appeared to have been sent out in bulk: The messages were not personalized and as such, appeared to have been sent out in bulk
- The messages did not have an unsubscribe option: It was not possible for the person receiving such messages to request the sender not to send such messages

However, since there is no legal definition of SPAM in the Kingdom of Saudi Arabia, the messages sent by the bulk SMS sender could not formally be classified as SPAM.

It would have been possible to initiate action against a Bulk SMS service provider or the beneficiary involved in such activities if the service provider or beneficiary had been based in Saudi Arabia, since the SMS Service Provider's Obligations within the Special Terms and Conditions of Type (B) Class License for Bulk SMS Service stipulate that:

- No message shall be sent to the subscriber without his approval
- All ads and/or promotional materials for the service shall contain numbers allocated only for the service advertised. Also, the cost of the message shall be written clearly and shown in the video ads, so that the beneficiaries can have adequate information before obtaining the services
- Any message shall be sent through licensed message centers and telecommunication networks in the Kingdom
- If the service provider is to use the Internet in sending and receiving the messages, all servers shall be based in the Kingdom etc.

While Clause 11 – Section 37 of the Telecom act prohibits “Misuse of technology to cause annoyance”, the definition of “annoyance” is not clear and as such it is not clear if such messages could be considered to be an annoyance and if so, the threshold (number of emails) that would qualify as an annoyance.

Since the Bulk SMS sender, in this case, is based outside the Kingdom and outside the jurisdiction of its Laws, it would only have been possible to prosecute/penalize them for sending SPAM if the Kingdom had a SPAM related agreement with the country in which the sender was operating in. However, since the Kingdom does not have any such SPAM related agreement in place currently, it was not possible to prosecute/penalize the sender.

If it were possible to trace the manner in which the SPAMmer obtained the mobile numbers to a local bulk SMS service provider or to a local telecom operator, it would have been possible to penalize the local bulk SMS service provider or to the local telecom operator, since Article 56 of the Telecom



Bylaws states that “A service provider shall not disclose information other than the user’s name, address and listed telephone number to anyone without the user’s written consent or unless disclosure is required or permitted by the Commission or by law to another legally authorized public authority” and Article 58 stated that “A service provider shall be responsible for user information and user communications in its custody or control and in that of its agents”.



5.4 CASE-3: MOBILE SPAM – 700 NUMBERS

Summary of the Case

This case was filed at CITC by a Saudi Telecom user complaining that he had repeatedly received an SMS on his mobile containing a link to a local 700 number. The SMS invited him to participate in a general knowledge competition and win various prizes, including cars and cash.

After receiving the invitation a number of times the user decided to participate by calling the advertised premium rate number. Following a number of calls to the advertised number, apart from not winning anything, his phone bill reached 5000 riyals and his line was disconnected.

The user registered a complaint with CITC on the grounds that:

3. The Company that sent the messages was not identified in the message.
4. The huge number of messages sent inviting him to participate caused him significant annoyance.
5. The competition probably did not offer any prizes, and instead only sought to make illegal financial gains from the premium rates by making the users repetitively call their 700 numbers.

The Approach Taken

Upon receiving the complaints by the user, CITC opened an investigation on the matter and called in the 700 services licensee's representative for questioning.

The investigation determined that the promotional SMS messages were being sent from outside Saudi Arabia. When interviewed, the 700 services licensee's representative denied all allegations about sending bulk SMS messages to promote their services, both directly from inside Saudi Arabia, or by hiring a cross border service provider. He also claimed those messages could be sent by competitors to damage his company's reputation.

The company's representative also stated that his company had been using a provisionally allotted 700 number for the purpose of competitions. However, they have recently stopped all further competitions using their provisional 700 number, since the formal approval for the 700 number is still pending.

The Action Taken

CITC decided that they were not able to prosecute the 700 service licensee under the existing laws of the Kingdom, specifically the Telecom Act and its subsequent bylaws.

CITC decided not to take the case any further, particularly since the company also confirmed that they no longer offered competitions using the 700 service number.

Analysis

Clearly, the messages sent to the user fall within the commonly used definition of SPAM, since it involved:

- Sending of unsolicited messages to the user
- Sending of messages that were promotional and commercial in nature

Given the lack of personalization of the messages, it could be assumed that the messages were sent out in bulk.

Since the SMS Service Provider's Obligations in the Special Terms and Conditions of Type (B) Class License for Bulk SMS Service states that "No message shall be sent to the subscriber without his approval", it would have been possible to prosecute the Bulk SMS service provider, if it were a local Bulk SMS Service provider.

<p>Final Version</p>	<p style="text-align: center;">Page 33 of 64 Confidential - Internal Use Only</p>	
-----------------------------	---	--



Since the Bulk SMS Service Provider is based outside the Kingdom, CITC would have been able to prosecute the service provider only if an international agreement existed with the country that the Bulk SMS service provider was operating in. Under the current circumstances, CITC can only request STC and Mobily to block all further SMSes from the identified Bulk SMS Service Provider.

The 700 service license agreement (Special Terms and Conditions of Type (B) Class Licenses for Audio Text Services) states that promotional messages sent to the user could only be sent through a CITC licensed bulk SMS service provider. If CITC could have proved that the 700 number licensee had authorized the sending of the promotional messages, it would have been possible to prosecute them. However, in this instance, the 700 number licensee denied having made such an authorization and CITC was also not able to establish the link between the two companies, thereby rendering this approach ineffective.

5.5 CONCLUSION

The three cases highlight the importance of being able to address SPAM through a well-defined policy framework that encompasses regulations, international agreements, well-defined enforcement mechanisms, industry initiatives etc. While a regulation focused on addressing SPAM in the Kingdom will go a long way in addressing the problem in the Kingdom, it will not suffice by itself.

The current laws in the Kingdom, including the cCrime Act, as well as the Telecom Act and its bylaws do not address the issue of SPAM in its entirety. Given the lack of a formal definition of SPAM in the Kingdom, it is not even possible to classify unsolicited messages as SPAM, in most instances.

While certain requirements have been addressed within the Licensing Agreements (e.g. the need for users' consent before sending unsolicited commercial SMS messages to them), no specific penalties have been defined within the licensing agreements or other law in the Kingdom (other than possible withdrawal of the license).

While the Telecom Act contains some conditions that could be used to prosecute perpetrators for offences that are similar to SPAM in nature, through the inclusion of a term on misuse of telecom facilities for causing "annoyance", it does not provide the proper definition or metrics to measure and identify what could be considered an "Annoyance".

While the Telecom Act does provide for privacy of personal information of subscribers of the telecom firm, there is no provision in any other law that prevents misuse of personal information for purposes other than the purpose it was collected by any agency.

The lack of international agreements to prosecute service providers, who send unsolicited commercial or objectionable messages from other countries, has also encouraged companies to send such promotional messages from other countries.

It is important to address the problem in its entirety through the use of effective legislation(s) that cover the issue in its entirety as well as through other policy initiatives focused on addressing other aspects of SPAM.



6 APPENDIX A: ANTI E-CRIME ACT

Article (1): Definitions

The following words and expression shall have the meaning assigned hereunder to each of them unless context requires otherwise:

1. Ministry or (MCIT): Ministry of Communications and Information Technology.
2. Minister: Minister of Communications and Information Technology.
3. CITC: Communications and Information Technology Commission.
4. Governor: Governor of Communications and Information Technology commission.
5. Person: Any natural or juridical person, public or private.
6. Computer: any computer or a system of computers processing or storing information.
7. Computer Output: Any printed or reproduced reports, or in any form resulted from computer.
8. Computer Services: Includes data processing, storage, recovery, and retrieval as well as computer timing.
9. Data: Includes information or concepts under preparation or previously prepared properly to be used in computer, and any thing that can be stored, processed, transferred, or established by computer, such as numbers, letters, codes, etc.
10. Electronic, Audio, Mechanical, or other Hardware: Any devices or tools used or usable to interrupt or disrupt the work of computer or any of its functions.
11. Computer Functions: Works / processes conducted through computer such as calculations, computations, processing of texts or data, deletion, retrieval, etc.
12. Disrupt or Interrupt Computer Operations: Cause disruption or interruption to computer operations and processing by accessing to, interfering with, or penetrating its information, taking a copy or more of data stored in it or deleting or altering such data, etc.
13. Software: Data that includes guidelines or applications, when operated in computer, it will perform the required function.
14. Information System: Software packages or tools prepared to process and manage data.
15. Information Network / Internet: Network connection between more than one information system to obtain or exchange information.
16. Site: A site where information are made available on the internet through a specific address (URL).
17. Receiving: View the information or obtaining it.

Article (2): Law Objectives

The IT Criminals Law aims at creating legal and regulatory standards to combat information, computer and internet crimes through specifying /determining the relevant crimes and punitive actions for each crime or violation, and determining the parties of jurisdiction to handle such crimes and enforce punitive actions, in order to affect the following.

- Maintain information security.
- Promote further increases in employment of computers and networks.
- Safeguard the intellectual rights of the legal use of computers and networks.



- Safeguard public interests, morals, and communal values.
- Develop and safeguard the National Economy through providing protection and security to information, computers and Internet.

Article (3)

Without project to any stronger penalty stipulated in the Law, a person who commits any of the following acts will be punished by imprisonment of no more than 5 years and a maximum fine of SR5 million or one of them:

1. Deliberately accessed – unlawfully - without having the right, a site or information system, with due consideration to purpose of such accession, so If he intends to delete, destroy, divulge, damage, alter or re-publish personal information, the minimum penalty shall be imprisonment for 2 years and a fine of SR500,000, or either one of them.
2. Forgery (falsification) of any document that was processed through an information system. This punitive action shall apply to any person who used the falsified document although he knows it is forged.
3. Access through an information network or a computer or through any similar means such as applications, software, etc, which may disrupt or interrupt the work of the information network, or destroy, delete, erase, disclose, damage or alter software or data used by or stored in the network, even if he does not manage to realized such a purpose lies behind his offence. However if he manages to realized the purpose, the minimum punitive action shall be imprisonment for 2 years and SR1 million or either one them.
4. Interrupt, disrupt, or interfere, deliberately and unrightfully, by any means through the information network, a computer or any similar means, access to services, hardware, software or information sources.
5. Produce, prepare, configure, transmit or store through an information network, a computer, or any similar means, any thing that may cause harm to public order or morals. If the action is directed toward an event, the minimum punitive action shall be imprisonment for 2 years and a fine of SR1 million or either one them.
6. Remittance or transference of illegal funds or hide their illegal source, or use, earn or possess funds although he knows that they are from illegal source, or transfer funds or properties although he knows their illegal source, through the information network or a computer or similar means to cause such funds to become legal, or build or publish a site to commit such actions.
7. Offend any religious or family principles or values or privacy of others through an information network or a computer or any similar means.
8. Build or publish a site on the information network or a computer or on a similar means to facilitate trading in human beings or dealing with them.
9. Build or publish a site on the information network or a computer or on a similar means for the purpose of smuggling or taking drugs or other mental affecting drugs or any similar items or facilitating dealing with such things.

Article (4)

Without prejudice to any stronger penalty stipulated by any other law, any person who commits any of the following crimes shall be punished by imprisonment for 2 years maximum and a fine of no more than SR1 million, or either one of them.

1. Take hold for himself or for a third party, through an information network, a computer, or a similar means, of cash money or a voucher or signing such a voucher utilizing a fraudulent way or a fake name or impersonation if such an action to deceive the victim.

Final Version	Page 36 of 64 Confidential - Internal Use Only	
---------------	---	--



2. Use the Information network, a computer, or similar means to access unlawfully and unrightfully to bank accounts, or a credit card information or alike, to utilize such information to obtain personal data, funds or services

Article (5)

Without prejudice to any stronger penalty stipulated by any other law, any person who commits any of the following crimes shall be punished by imprisonment for maximum of 2 years and a fine of maximum SR500,000 or either one of them.

1. Unlawfully and unrightfully eavesdropping (listening), receiving or intercepting data sent over an information network, a computer or similar means.
2. Utilizing an information network, a computer or alike to threaten or blackmail any juridical or natural person compelling him to act or enact, even if the action or inaction is lawful, or for the purpose of earning money or other benefits.
3. Access unlawfully to a site of a juridical or natural person to alter its design, delete, tamper, history or revise its information, occupy its address or obtain confidential information from it.

Article (6)

Without prejudice to any stronger penalty stipulated by any other law, a person who commits any of the following crimes shall be punished by imprisonment for maximum of 10 years:

1. Build or publish a site on an information network or a computer or similar means for a terrorist group under falsified names to facilitate connection with its leaders or members, promote their thoughts, financing their activities, publishing information on how to produce/make/prepare burners, explosives, or any other tools used in terrorism acts.
2. Access deliberately and unlawfully to any site or system, directly or through an information network, a computer or similar means to obtain data that harm the country's internal or external security or national economy. If access is for deleting such data or information, damage or destroy such data, or transmit harmful ideas or thought, the minimum limit of punishment will be imprisonment for 3 years.

Article (7)

Should a person commit any of the crimes stipulated in this Law during performance of his job or as a result of it, or facilitate the crime to others, he will be punished by imprisonment of 5 year minimum and a fine not less that SR1 million, or either one of them.

Article (8)

A person who provoked or assisted others or agreed with them to commit any of the crimes stipulated hereunder, and the crime was committed accordingly, he will be liable for the full punishment stipulated for such a crime. However, if the crime has not occurred, he will be liable for half of the punishment stipulated for such a crime, if committed.

Article (9)

Any person who started committing any of the crimes stipulated in Articles 3,6,7,8,9 will undergo half of the punishment stipulated in the Law.

Article (10)

The Private and publish authorities and entities shall take internal precautionary and control measures to safeguard their own information networks, detect occurrence of the crimes stipulated in this Law, thwart such crimes, and comply with the instructions, and technical specifications issued by CITC in this regard.



Article (11)

The private and public authorities/entities, upon having sufficient signs or evidence of penetrating their own information network shall promptly take the following actions:

1. Notify CITC promptly of such penetration.
2. Prepare a report containing available data and information on the relevant penetration and forward a copy to CITC.

Article (12)

Without prejudice to the rights of bona-fide parties, In all cases, all hardware, software and other means used in committing the crimes stipulated in this law shall be confiscated as well as they money earned from such unlawful acts. Further, the decision shall include permanent or temporary closure of the site or project, which was the source of the relevant crimes, if the crime is committed at knowledge of their owner, as determined by the party of jurisdiction, and according to its decision

Article (13)

The General Investigation and Prosecution Commission may require preventing any person from leaving the kingdom, who proved to be involved in such violation until such time.

Article (14)

CITC shall receive notification, investigate, control and inspect any crimes under this Law and prepare a record of such crimes. CITC shall have the right to seize the hardware, software and systems utilized in committing such criminal acts until the issue is decided. CITC Governor shall determine the persons who will be assigned to perform the task and the methods of performing the control and inspection procedures.

Article (15)

Having finalized its investigations, the Crime Investigation Record stipulated in this Law shall be forwarded to the General Investigation and Prosecution Commission for investigation and prosecution according to its Law.

Article (16)

The Board of Grievances is responsible for consideration and decision with regard to any violations to the provisions of this Law.

Article (17)

Any Person who sustained harm as a result of committing or start committing crimes mentioned in this Law, shall have the right to file a case to the competent arbitrary bodies to claim for compensation against the harm he sustained.

Article (18)

The Minster shall issue the implementing regulations of this Law based on CITC proposal, within 120 days as of its publishing date in the Official Gazette.

Article (19)

This Law shall go into effect after 120 days of its publishing in the Official Gazette.



7 APPENDIX B: ETRANSACTIONS LAW – DRAFT VERSION

CHAPTER – 1 GENERAL PROVISIONS DEFINITIONS

ARTICLE – 1

The following words and expressions shall have the meanings hereby assigned to them unless the text requires specifically otherwise:

Ministry/ MCIT: The Ministry of Communications and Information Technology.

Minister: The Minister of Communications and Information Technology.

CCIT: The Commission of Communications and Information Technology

Governor: The CCIT Governor.

Portfolios: CCIT Portfolios.

The By-Laws: The Executive Regulation of this Law.

Person: Any natural or judicial person, whether private or Public.

National Center: The National Center for Digital Certification, the authority that is committed to organize the certification processes and use the digital certificates in the Kingdom.

Electronic: The technology of using any electrical, electromagnetic or optical means, or any similar means of technology.

Electronic Transactions: Any interchange of information, correspondence, contracting, or any other action that is partially or wholly made or executed by an electronic means. The singular is an electronic transaction.

Electronic Data: Any text, image, sound, code, drawing, etc in electronic format, individually or collectively.

Electronic Data System: An electronic machine or program used to initiate, generate, send, transmit, deliver, store, display, or process electronic data.

Electronic Record (Register): Electronic data initiated by an Electronic Data System, which is retrievable in understandable manner, and used in Electronic transacting.

Electronic Signature: Electronic data included in an electronic transaction, or added to it or logically associated with it, acts in lieu of a hand signature, and may be used for proving the signer's identity as well as his approval on the transaction, and detection of any amendment to the transaction after its signature.



Electronic Signature Initiation System: An electronic data system, prepared in a way to act either independently or mutually with another electronic data system to initiate an e-signature.

The Signer: The person who has an Electronic Signature Initiation System and makes an electronic signature, or has someone to sign electronically on his behalf using such a system.

Electronic Signature Verification Data: Electronic data such as codes or encryption keys used to verify the validity of the electronic signature.

Digital Certificate: An electronic Register issued from an electronic certification services provider, used to confirm the identity of the certificate owner and include his signature verification data, which meets all provisions of this Law and its By-Laws.

The Initiator: The person who sends an electronic transaction by himself or on behalf of somebody else. The mediator is not deemed as an initiator of the electronic transactions.

The Recipient: The person to whom the electronic transaction is sent, and this does not include the mediator.

The Mediator: The person whose work is to convey the electronic transaction to another person, or to deliver such a transaction, or perform other services relating to the electronic transaction.

Certification Services Provider: The person who is licensed to issue digital certificates or provide another service or mission relating to that or to the electronic signatures according to this Law.

Encryption: A process that leads to transforming the form of electronic data into another form which is different from the original one to prevent unauthorized persons from viewing the data and realizing their contents.

OBJECTIVES OF THE LAW AND SCOPE OF IMPLEMENTATION

ARTICLE – 2

The following

This Law organizes The electronic transactions and signatures to the following effects:

1. Set unified regulatory standards to use electronic transactions and signatures and streamline their usage in the private and public sectors through reliable electronic registers.
2. Enhancing confidence in the soundness and validity of electronic transactions, signatures and records.
3. Facilitating usage of electronic transactions locally and internationally to benefit from them in all fields such as e-government, trading, medicine, education and e-payments.
4. Eliminating any barriers in using electronic transactions and signatures.
5. Preventing misuse of electronic transactions and signatures and related fraud.

ARTICLE – 3

Final Version	Page 40 of 64 Confidential - Internal Use Only	
----------------------	---	--



The following transactions shall be excluded from this Law:

1. Transactions relating to the Personal Status Law such as marriage, divorce and will (testament).
2. Issuance of deeds relating to real estate transactions.

Unless the competent authorities issue instructions that allow their electronic transactions based on certain controls agreed upon with MCIT.

ARTICLE – 4

1. The Law does not oblige any person to do electronic transactions without his agreement. Such an agreement may be explicit or implicit.
2. With due consideration to the conditions placed by the government body regarding electronic transactions, its acceptance of electronic transacting must be explicit.
3. Any party willing to enter into electronic transacting may place additional conditions relating to it for accepting electronic transacting and signatures, providing that such conditions shall not contradict with the provisions of this Law.

CHAPTER – 2

LEGAL EFFECTS OF ELECTRONIC TRANSACTIONS AND SIGNITURES

ARTILE – 5

The Electronic Register and the electronic signature shall constitute a valid legal proof and shall not lose their legal effect. They may not be invalidated or rejected as an executable evident merely because they are entirely or partially electronic, once their details can be viewed in the initiator's electronic data system, and they indicate how such details can be viewed.

ARTILE – 6

1. If any Law in the kingdom stipulates, for any reason, other than what is indicated in Article-3 of this Law, to maintain or submit a record, or stipulates that the record shall be in writing, then this condition will be realized when the record is in electronic format, providing that.
 - a. The electronic record shall be stored in a manner that enables its usage and to revert to it later.
 - b. The electronic record shall be stored in its originally initiated, sent or received form, or in a form that proves that its content is identical with the form in which it was initiated, sent or received.
 - c. The electronic data which enable identification of the initiator, the sending party, sending and receiving date and time shall be stored with the electronic register.
2. Any person may meet the requirements stipulated in paragraph-1 of this Article, at his own responsibility, by using the service of another person,
3. The By-Laws (Executive Regulations) will specify the storage procedures of electronic records, the conditions for presenting them in their electronic from, and the conditions and controls for viewing them.



ARTILE – 7

1. The electronic record is deemed as an original when technical means and conditions are used to ensure that its information has not been altered since its initiation or after its final approval, and allow for retrieval of such information at any later time. The Executive Regulations will specify the regulations and conditions.
2. Any addition or illustration introduced to the electronic record in the light of normal conditions of electronic and non-electronic transactions will not be considered as a violation to the electronic origin.

ARTILE – 8

- 1) The electronic transaction, including the electronic signature, will be accepted as an evident if the electronic record fulfills the provisions of Article-7 of this Law.
- 2) Electronic transacting, including electronic signature, may be accepted as a supporting evident even if the electronic record does not fulfill the provisions of Article-7 of this Law.
- 3) Upon estimating the validity of electronic transacting as a supporting evident, the trust in the following factors shall be taken into consideration;
 - a. The method used in initiating, saving and informing the electronic record and the possibility of revising it.
 - b. The method used to maintain security of information.
 - c. The method in which the identity of the initiator is determined.

CHAPTER – 3

ELECTRONIC SIGNATURE

ARTILE – 9

If any law in the kingdom stipulates a manual signature on a document or a contract, etc., then the digital signature affixed according to this system, shall be deemed to satisfy this condition, and shall be considered as a manual signature and have all relevant legal effects.

ARTILE – 10

The electronic signature is considered to be valid and fulfills all provisions of the Law in the following cases:

1. The signature initiation data shall be relevant to the signer himself.
2. The signature initiation data, at the time of signature, shall be under the control of the signer.
3. It shall be possible to detect any alternation to the electronic record or the electronic signature after making the signature.

ARTILE – 11

1. Whoever wishes to make an electronic signature, he shall do this according to the regulations, controls, conditions and specifications provided for in the By-Laws. He shall observe the following:

Final Version	Page 42 of 64 Confidential - Internal Use Only	
----------------------	---	--



- a. Take the necessary measures to avoid any illegal usage of the electronic signature initiation data or the personal equipment relating to his signature.
 - b. Notify the certification services provider or any person who may depend on the signature about any illegal usage of his signature according to the By-Laws procedures.
 - c. Provide accurate information to the certification services provider and any person who may rely of his electronic signature.
- 2 Any one who depends on the electronic signature of another person shall exert a reasonable and recognizable effort to verify the validity of the signature by using the electronic signature certification data as per the By-Laws procedures.

ARTICLE – 12

Should the electronic signature fails to meet the conditions and provisions stipulated in this Law, the validity condition stipulated in clause 4 shall not apply to electronic transacting or signature.

Note from translator: this is not clear.

CHAPTER – 4

VALIDITY OF ELECTRONIC TRANSACTING

ARTICLE – 13

Acceptance in contracts may be expressed through electronic transacting and the contract in this case is considered valid and executable as long as it is made according to the provisions of this Law (unless it is proven otherwise). The contract will not lose its validity or applicability merely because it was made by one electronic record or more.

ARTICLE – 14

- 1) Contracting may be made through automatic or direct electronic data systems, i.e. between 2 electronic data systems or more, which have been prepared and programmed in advance to perform such tasks and represent the contract parties, The contract will be valid and of legal effect, although there has been no direct interference by any natural person in the contracting process.
- 2) A contract may be made by an electronic data system and a natural person, if the person knows, and supposedly he knows, that he is transacting with an automatic system which is assigned to execute the contract.

ARTICLE – 15

The electronic record is considered as being sent by the initiator if he sends it himself or by an authorized representative or through any automatic system programmed by the initiator to act automatically on behalf of him. The mediator shall not be considered as an initiator of the record.

ARTICLE – 16

- 1 Unless otherwise agreed between the initiator and the recipient, the electronic record is considered to have been sent once it enters a data system that is not under control of the

Final Version	Page 43 of 64 Confidential - Internal Use Only	
----------------------	---	--



initiator or the person on behalf of whom the record was sent. The Executive Regulations demonstrate the technical criteria of the data system and the method of defining the time and location of the electronic record or receiving it.

- 2 If the initiator stipulates to get an acknowledgement of receipt from the recipient, the electronic record shall not be deemed as has been sent until the receipt is received.
- 3 The acknowledgement receipt is subject to the conditions provided for in the Executive Regulations.

CHAPTER – 5

MCIT AND CCIT RESPONSIBILITIES

ARTICLE – 17

Implementation of this Law shall be overseen in the following manner:

1. The ministry will define the general polices, draw the plans and developmental programs for the electronic transactions and signatures, raise the projects and any proposed revisions, coordinate with the government bodies and other parties with regard to implementing this Law, and represent the kingdom in local, regional and international organizations with regards electronic transactions and signatures. The Ministry shall have the right to authorize the CCIT and other bodies for representation.
2. The CCIT shall implement its relevant parts of the Law, follow up and monitor the implementation of the Law by other parties. It shall have the following authorities to this effect:
 - a. Issuance of Licenses for "Certification Services Providers" in the kingdom, determine the obligations of the Licensee, renew/ suspend/ cancel the licenses and verify compliance of services providers with their licenses as well as with the provisions of the Executive Regulations of this Law and the CCIT resolutions.
 - b. Take the necessary actions to ensure continuation of services provided to persons who are dealing with the certification services providers whose services have been suspended or cancelled or their licenses not renewed. The Executive Regulations shall determine the relevant procedures for this.
 - c. Determine the licensing fees of the Certification services provider after securing the Minister's approval on this.

ARTICLE – 18

All CCIT, Ministry and the National Center's employees shall be obliged to maintain confidentiality of information which they may become aware of because of their work. Information may not be disclosed to any person for any reason unless provided for in the Law.



CHAPTER – 6

NATIONAL CENTER FOR DIGITAL CERTIFICATION AND CERTIFICATION SERVICES
PROVIDERS

ARTICLE – 19

The National Center for Digital Certification will supervise the tasks relating to management of digital certificates, coordinate the matters relating to the standards and specifications, propose regulations and polices to organize the Center's work, and develop the usages of digital certificates in the Kingdom. The Executive Regulations will define how the Center works and its relevant controls.



ARTILE – 20

- a. The National Center, through the Ministry, will coordinate with the external parties that are conducting works similar to the Center, for mutual recognition of the electronic certificates issued from the other party.
- b. The Center will define the technical specifications for the Certificates Issuance System, certificate contents and form, electronic signature initiation process, and its documentation system.
- c. The Center will determine the controls for issuance, sending, maintaining and cancellation of digital certificates.

ARTILE – 21

Based on Article – 17, paragraph (a), digital certificates issued from any other country will be treated as if they are issued from the Kingdom.

ARTILE – 22

Any party willing to be a certification services provider must obtain the required license from the CCIT before conducting this business. The Executive Regulations will illustrate the conditions and procedures for obtaining the license, its period, renewal, assignment, licensee's obligations, licensee's suspension of services and procedures and consequences of such suspension.

ARTILE – 23

The certification services provider shall comply with the following:

- 1) Issue, deliver and maintain digital certificates according to his license and the controls and procedures set forth in the Executive Regulations.
- 2) Use reliable tools for issuance, delivery and safekeeping of digital certificates, and take all necessary measures to protect them from falsification or tampering according to the Executive Regulations and his license.
- 3) Establish a data base for the certificates he issues, maintain all original data and revisions thereto including the suspended and cancelled certificates, and allow all users to view such data electronically at any time.
- 4) Maintain, with all his subordinates, the confidentiality of information which he obtains due to the nature of his business, except for the information allowed by its owner to be published or disclosed, or in the cases provided for in the Law.
- 5) Take the personal information directly from the certificate applicant, or from a third party providing that an explicit approval shall be taken from the applicant.
- 6) Issue the certificate containing the data required by the Executive Regulations and complying with the conditions of Systems Security and Protection and the Digital Certificates Standards laid down by the National Center.
- 7) Obtain prior approval from the CCIT before stopping the provision of services or assigning his license, as per the procedures included in the Executive Regulations.
- 8) Deliver all documents and information with him to the CCIT in all cases of suspension of services, so they will be dealt with in accordance with the provisions and procedures of the Executive Regulations.



ARTICLE – 24

The Certification Services Provider will be held responsible for the accuracy of the certification information included in the certificate upon its delivery and the validity of relationship between the certificate owner and its electronic data. He will be held responsible for any harm sustained by any person because he trusted such information in good faith.

ARTICLE – 25

- 1) The certification services provider must cancel the certificate or suspend it upon request of its owner or in the cases determined by the Executive Regulations. He shall promptly notify the Certificate's owner of such cancellation or suspension and its cause, and immediately stop the action if the cause does not exist any more.
- 2) The certification services provider will be held responsible for any harm sustained by any person if the provider fails to stop or cancel the digital certificate after he has received clear instructions from the certificate's owner

CHAPTER – 7

RESPNSIOBILITIES OF THE CERTIFICTE OWNER

ARTICLE – 26

- 1) The certificate's owner will be responsible for the security and confidentiality of his electronic signature initiation system, and any usage of this system will be considered as initiated by him. He shall comply with the conditions of his certificate usage and his electronic signature initiation.
- 2) The certificate's owner shall notify the certification services provider of any revision to the certificate information or if it is disclosed and become no more confidential.
- 3) The suspended or cancelled certificate's owner shall not have the right to use the electronic signature elements of that certificate with another certification services provider. The Executive Regulations will define the procedures to prevent such occurrence.

CHAPTER – 8

VIOLATIONS AND PENALTIES

ARTICLE – 27

The Certification Services Provider will be judged non-compliant in the following cases:

- 1) If he conducts business without payment of the license fees or any other due payments to the CCIT, failure to conduct business within 1 year after obtaining the relevant license,

Final Version	Page 47 of 64 Confidential - Internal Use Only	
----------------------	---	--



assignment of the license without approval of the CCIT, or failure to comply with any other license regulations.

- 2) If he utilizes the information gathered on the certificate applicant for other purposes beyond the certification activities without approval of the owner.
- 3) If he discloses the information he is given access to because of the business, unless it is allowed by the Law or permitted in writing by the certificate's owner.
- 4) If he misuses the certification services
- 5) If he provides false or invalid information to the CCIT.

ARTICLE – 28

- 1) A committee or more will be formed of 3 members from CCIT or others, by a resolution from the Governor, providing that one of them at least shall be a legal advisor. The formation resolution shall stipulate for a spare member and determine the remunerations of the members. The committee shall use the services of technical specialists as it deems proper.
- 2) The above mentioned committee shall look into the violations mentioned in Article 23 and investigate the certificate owner complaints with regard to suspension or cancellation of their certificates by service providers or their refusal to issue certificates for applicants. The violator may be subject to the following penalties by the committee:
 - a. Suspension of the license.
 - b. Cancellation of the license.
 - c. A financial penalty of SR 500 maximum.

ARTICLE – 29

Without prejudice to Article 23, any provider who commits any of the following acts will be considered noncompliant:

1. Conducting business (provision of certification services) without a license from the CCIT.
2. Forging electronic files, electronic signatures, or electronic digital certificates, or misusing such things when he knows that.
3. Illegal entrance for any reason to any electronic system or software, or maintaining an illegal connection with such systems.
4. Preventing completion of electronic transactions by any altering, erasing, spoiling or destructing data or deactivating data systems, etc.
5. Manipulating the data of any electronic information system by addition, deletion, modification or destruction.
6. Interrupting the functions of an e-data system, or deactivating it.
7. Misusing electronic transactions for any purpose against the disciplines of Islamic Shari'a Law or general ethics.
8. Providing purposeful erroneous information to the certification services provider or false information on the electronic signature to any party who trusted the signature by Law.
9. Entering the e-signature initiation system of any other person without a valid authorization, or if he copies, reforms or dominates such a system.



10. Initiating, publishing, falsifying or using an e-signature certificate for a malicious or any other illegal purpose.
11. Impersonation of another person's identity, or falsely claim that he is authorized to request or accept the certificate or suspend or cancel it.
12. Publishing a false, invalid, cancelled, or suspended certificate, or enabling access by another person to it although he knows its status. Excluded from this are the rights of the Certification Services Provider included in Article 19, paragraph 3.
13. Any other action that contradicts with the Law and its Executive Regulations and any implementing regulations thereto.

ARTICLE – 30

Without prejudice to any stronger penalty provided for in any other law, any one who commits any of the violations indicated in Article 25 of this Law, shall be subject to a penalty not exceeding SR 5 million or 5 years imprisonment or both penalties. The judgment may include confiscation of the hardware, systems, software used in the violation and cancellation or suspension of the services provision license. The Grievance Board will be the competent body to give such a decision.

ARTICLE – 31

The CCIT, in cooperation and coordination with the relevant authorities, will control and inspect the violations to the Law and prepare a minutes on this. The CCIT shall have the right to retain the hardware, systems and software used in the violation until a resolution is taken in this regard. The Governor will determine by a resolution the names of persons who will attend to this task and how to conduct inspection and control procedures.

ARTICLE – 32

The Violations control Record indicated in Article 25 will be transferred to the Public. Investigation and Prosecution Authority for investigation according to its regulations.

ARTICLE – 33

Any person who sustained harm from violations or crimes under this Law or failure to comply with Law, and its controls and obligations, shall reserves his right to institute action before the competent judicial authorities to claim for indemnity against such harm.

CHAPTER – 9

CONCLUDING TERMS

ARTICLE – 34

Compliance with this Law shall not contradict with the relevant provisions of the intellectual property rights and other international agreements in which the kingdom is a party.

ARTICLE – 35

The Minister will issue the Executive Regulations of this Law within 120 days from its publishing date, and will be published in the official Gazette.

ARTICLE – 36

Final Version	Page 49 of 64 Confidential - Internal Use Only	
----------------------	---	--



The Law will go into effect after 90 days of being published in the Official Gazette.



8 APPENDIX C: TELECOMMUNICATIONS ACT

Telecommunications Act

Chapter One

Definitions

Article One:

Whenever mentioned in this Act and its Bylaws, the following terms and expressions shall have the meaning hereunder assigned to them unless otherwise specified:

Kingdom:	The Kingdom of Saudi Arabia.
The Act:	The Telecommunications Act.
The Bylaws:	The Bylaws of the Act.
The Ordinance:	Ordinance of Saudi Communications Commission.
The Ministry:	The Ministry of Post, Telegraph & Telephone.
The Minister:	The Minister of Post, Telegraph & Telephone.
The Commission:	The Saudi Communications Commission.
The Board:	The Board Of the Saudi Communications Commission.
Telecommunications:	The conveyance of signals between defined termination points by wire wireless equipment, including the conveyance of signals over the Internet.
Telecommunications Services:	Conveying and routing of signals “in whole or in part” over the public Telecommunications networks including T.V& Radio Transmission and Internet services.
Telecommunications Network:	The systems used for provision of telecommunication services, including switching equipment, cables, towers, wireless equipment, optical, electromagnetic or any other telecommunications means and the associated equipment.
Universal Service:	Provision of the minimum level of



Universal Access:	telecommunications services with adequate quality and at affordable prices to all users. Provision of opportunity to all users in the kingdom to utilize the minimum level of the adequate quality telecommunications services within a specific geographical area and at affordable prices.
The Operator “Service Provider”:	Any licensee providing public telecommunications service or operating telecommunications network used to provide such service.
Dominant Operator:	The operator whose service covers at least 40% of specific telecommunications market in the Kingdom, unless the Commission decides to change this share according to the market situation.
The User:	A natural or juridical person who uses the telecommunications services.
Frequency:	Number of cycles per second of a radio wave.
Frequency Spectrum:	The frequency bands that can be used in Radio Communication according to International Radio Regulations.
National Frequency Spectrum Plan:	The plan prepared by the Commission and approved by the Council of Ministers for allocation of the frequency spectrum usage to the concerned parties.
Numbering:	It is a serial numbering pattern to identify designated termination point in the public telecommunications network, and includes the necessary information for routing of the telecommunication signals to this termination point.
National Numbering Plan:	The plan prepared by the Commission to specify the scheme of numbers used in various telecommunications services.



Chapter Two
General Provisions

Article Two:

The supervision of the Telecommunications Sector shall be as follows:

1. The Ministry shall make the general policies, plans and development programs for the telecommunications sector, submit applications for granting licenses as stipulated by this Act, its modifications and any amendments, coordinate with the concerned parties in respect of services provided to the government agencies, represent the Kingdom in domestic, regional and international bodies in the telecommunications sector and, at its discretion, delegate such representation to the Commission and other parties, approve the basis, principles and conditions relating to the Universal Service and the Universal Access as proposed by the Commission.
2. The Commission shall perform the functions and duties conferred upon it under this Act, the Bylaws and the Ordinance.

Article Three:

The Telecommunications Sector shall be regulated under this Act and pursuant to the following objectives:

1. To provide advanced and adequate telecommunications services at affordable prices.
2. To ensure the provision of access to the public telecommunications networks, equipment and services at affordable prices.
3. To ensure creation of favorable atmosphere to promote and encourage fair competition in all fields of telecommunications.
4. To ensure effective and interference-free usage of frequencies.
5. To ensure effective usage of National Numbering Plan.
6. To ensure clarity and transparency of procedures.
7. To ensure principles of equality and non-discrimination.
8. To safeguard the public interest and the user interest as well as maintain the confidentiality and security of telecommunications information.
9. To ensure transfer and migration of telecommunications technology to keep pace with its development.

Article Four:

The fixed and mobile telecommunication services shall only be provided through joint-stock companies that place their stock for public subscription.

Final Version	Page 53 of 64 Confidential - Internal Use Only	
----------------------	---	--



Article Five:

The license for provision of fixed and mobile telephone services is subject to the Council of Ministers' approval.

Article Six:

Necessary fees shall be paid in favor of the General Treasury for commercial provision of services, issuance of licenses to operators and permits for frequency usage as per the decree of Council of Ministers.

Article Seven:

The Commission shall set the principles and criteria for determining the telecommunications services fees in keeping with the competitive situation and the Bylaws shall state the necessary and relevant provisions.

Article Eight:

The Universal Service and the Universal Access requirements shall apply according to the principles and criteria stipulated by the Bylaws.

Article Nine:

The privacy and confidentiality of telephone calls and information transmitted or received through public telecommunications networks shall be maintained. Disclosing, listening or recording the same is not permitted, except for the cases stipulated by the relevant Acts.

Article Ten:

The Commission shall provide the necessary protection to the users and operators. The Bylaws shall specify the procedures for settlement of disputes arising among the operators themselves or between operators and users, including objection by users to billed amounts or the quality of the offered service.



Chapter Three

Frequencies

Article Eleven:

Frequency Spectrum is a state-owned natural resource. The Council of Ministers is the approving authority of the National Frequency Spectrum Plan for the purpose of achieving optimum utilization of this national resource, in accordance with International and Regional Agreements and approved regulations and standards.

Article Twelve:

The Commission shall regulate the frequencies as follows:

1. The Commission shall set the National Frequency Spectrum Plan in coordination with the involved parties, refer the same to the Ministry, for submission to the Council of Ministers for approval.
2. The Commission shall ensure that the frequencies are used in conformity with the National Frequency Spectrum Plan. Further, it shall set a special register called “National Frequency Register” to record all the information pertaining to the frequencies, their allocation and usage.
3. The concerned parties, as per their responsibilities, shall manage and supervise their assigned frequencies. The frequencies shall be used only for the purpose for which they are assigned.
4. The Commission shall manage and supervise frequencies assigned for civil and commercial purposes. It shall set a plan for distribution and usage of these frequencies, and shall submit the same to the Minister for approval.

Article Thirteen:

Any frequency allocated for civil or commercial purposes shall not be used by any user or operator without prior assignment by the Commission, obtaining the necessary license and payment of fees for usage of this frequency pursuant to the procedures prescribed by the Bylaws.

Article Fourteen:

In the event the frequencies are used in a manner contradicting this Act, its Bylaws or the licensing provisions, the Commission shall have the right to issue a decision to cease operation of the equipment used in violation or withdraw the same from service and resort to security authorities to enforce the decision if need be.

Chapter Four

Final Version	Page 55 of 64 Confidential - Internal Use Only	
----------------------	---	--



Numbering

Article Fifteen:

The Commission shall set the National Numbering Plan, and shall be responsible for the plan structure and management in order to meet the operators and users requirements pursuant to the procedures stipulated by the Bylaws.

Article Sixteen:

The Commission shall determine the conditions, the usage licensing procedures and fees, which shall be applicable to the assignment of numbers.

Article Seventeen:

The Commission shall have the right to modify the numbering scheme in the National Numbering Plan, provided that operators and users are given adequate notice prior to the implementation date of such modification.

Chapter Five

Licenses

Article Eighteen:

Anyone who fulfills the conditions and has the interest to provide Telecommunications service should submit his application to the Commission in order to obtain the license. The Commission shall issue the license according to the provisions of the Act and the Bylaws. The operators shall adhere to the conditions stated in the license issued to them.

Article Nineteen:

No license shall be required from the Commission for the establishment of a private internal telecommunication network with a limited capacity for the interconnection between the parts of a one facility like hospitals, residential compounds and hotels. This network shall not be interconnected with the public telecommunication networks unless an approval is obtained as per rules and procedures under the Bylaws.



Article Twenty:

1. Licenses shall be renewed by a decision of the Board. The relevant standards, rules and procedures shall be specified under the Bylaws.
2. The Board has the right not to renew, amend, suspend or revoke the license according to the rules, procedures and reasons stated in the Bylaws including the following reasons:
 - a. Repeated violation of a basic licensing condition.
 - b. Failure to pay licensing or other fees required by the Commission.
 - c. Repeated failure to comply with duly issued decisions of the Commission.
 - d. Failure to operate under the license within one year from the date of its issue.
 - e. Carrying out activities prejudicial to the public interest.
 - f. Bankruptcy, dissolution or liquidation of the licensee.
 - g. Re-assignment of the license without the consent of the Commission.

Exempted are the licenses pertaining to the provision of the fixed and mobile “Al Jawal” telephone services, for which the decision of the Board has to be approved by the Minister.

3. In the event that the license is not renewed, suspended or revoked, the Commission shall make such arrangements as are necessary to ensure continuity of service according to the rules and procedures under the Bylaws.

Article Twenty-one:

The Commission shall classify and identify the types of licenses and establish the conditions required for issuance of each type.

Article Twenty-two:

The Commission shall state on the licenses issued to operators the requirement for the issuance of bills, inquiry services and emergency services that should be provided according to the rules and procedures under the Bylaws.

Article Twenty-three:

The Board consent shall be obtained before the re-assignment of the license except for the licenses concerning the provision of the fixed and mobile “Al Jawal “ telephone services, for which the Board decisions are subject to the approval of the Minister. The Commission shall issue its decision in this regard within a reasonable period as identified in the Bylaws.



Chapter Six
Competition Rules

Article Twenty-four:

Subject to the rules of Articles Twenty-five and Twenty-six, operators are prohibited to enter into agreements with each other to undertake practices that would create a dominant operator for a certain telecommunications market or prevent, restrict or distort competition. The provisions of these agreements or decisions dealing with this matter will be considered null and void. The Bylaws specify the decisions and practices that would restrict competition and the actions to be taken in this regard.

Article Twenty-five:

1. Operators shall obtain the Board's approval before undertaking any merger with other internal or external operators, and shall inform the Commission within five working days of any initial agreement reached in this regard. However the Board's decisions on mergers pertaining to the provision of the fixed and mobile "AlJawal" telephone services shall be subject to the Minister's approval.
2. Operators or any natural or juridical person shall obtain the Board's approval before purchasing 5% or more of the shares or stocks of another operator licensed to work in the Kingdom or a percentage that creates a dominant position in a certain telecommunications market.
3. The Commission shall issue the appropriate decision regarding clauses "1" and "2" of this article within a reasonable period identified in the Bylaws.

Article Twenty-six:

Any operator dominating a certain telecommunications market or part of it, shall not undertake any activities or actions which are considered an abuse of his position. The Bylaws state the dominant operators' obligations and the rules by which a dominant operator's activity is considered an abuse.

Article Twenty-seven:

The operators shall ensure the transfer of numbers according to user requirements. The Bylaws state the associated procedures and conditions.



Chapter Seven

Interconnection

Article Twenty-eight:

The Commission shall establish the terms governing public networks access rights, the interconnection points and the interconnected operators' obligations.

Article Twenty-nine:

Each operator has the right to negotiate with other operators the agreements for interconnection with their telecommunications networks and services.

Article Thirty:

In the event that the concerned parties fail to reach an interconnection agreement according to Article Twenty-nine, they have the right to appeal to the Commission to settle the dispute. The Commission decision is binding on all parties.



Chapter Eight **Equipment and Facilities**

Article Thirty-one:

The Commission shall undertake all the necessary procedures to ensure the compliance of the terminal equipment and facilities used in the telecommunications network with the identified technical specifications, including the requirements of installation, operation and maintenance processes.

Article Thirty-two:

1. A license should be obtained from the Commission for the telecommunications equipment to be used in the Kingdom.
2. Telecommunications equipment shall not be used in a way that violate the provisions of this Act or pose any risk to various means of transportation or to their passengers.

Chapter Nine **Use of Properties**

Article Thirty-three:

All operators enjoy equal right of access to public and private properties for the purpose of providing telecommunications services. The Bylaws state the associated conditions and procedures.

Article Thirty-four:

The operators after obtaining the approval of the property owner or his representative could enter the property and use it within the necessary limits for purpose of the construction, operation and maintenance of telecommunications network.

Article Thirty-five:

If an operator fails to reach an agreement with the property owner or his representative as to the amount to be paid in respect of the acquisition or usage of that property, or for any other reasons, the operator may submit a request to the Commission for the expropriation of the property. The Commission may approve his request, if warranted, according to the provisions of the Expropriation Regulations.



Article Thirty-six:

The Bylaws state the rules governing the construction, operation and maintenance of the telecommunications networks, the operator's co-location at installations sites, and the protection of sites which are environmentally or historically significant.



Chapter Ten

Violations and Penalties

Article Thirty-seven:

Any of the following actions by any operator, individual or a juridical person constitutes a violation:

1. Providing telecommunications service or establish, operate or use a public telecommunications network without obtaining a license from the Commission.
2. Interconnection of a private internal network with a public telecommunications network without obtaining the necessary approval.
3. Failure to comply with an order issued by the Commission.
4. Use of any telecommunications equipment for the purpose of causing harmful interference with any other communications or exposing to risk different means of transportation or their passengers.
5. Use of any telecommunications equipment not licensed by the Commission.
6. Use of any frequency without a license from the Commission.
7. Interception of any telephone call or data carried on the public telecommunications networks in violation of the provisions of this Act.
8. Providing false statements or misleading information to the Commission.
9. Failure to obtain the Commission's approval before purchasing 5% or more of the total shares or stocks of an operator licensed to work in the Kingdom or a percentage that creates a dominant operator in certain telecommunications market in the Kingdom.
10. Failure to obtain the necessary approval according to the terms of the Act before merger with other operators.
11. Misuse of telecommunications services, such as causing damage to the public telecommunications networks or intentionally place a message of an indecent or menacing nature or which causes panic or disturbance.
12. Import, market or use telecommunications equipment not complying with the approved technical specifications.
13. Other than in the course of duty, intentional disclosure of any information or contents of any message, which has been intercepted in the course of its transmission.
14. Any other practice violating the provisions of this Act.

Article Thirty-eight:

1. Without prejudice to any more severe penalty stated in another Act, any person who commits any of the violations stated in Article Thirty-seven shall be subject to a penalty not exceeding SR 5 million.
2. The penalties mentioned under Clause "1" of this Article shall be proportionate to the violation committed and to the gravity of the violation in each individual case and will be imposed by a committee formed by a decision of the Board based on the nomination of the Commission Governor. The committee shall consist of 5 members from the Commission employees or others including at least one official advisor. The committee shall issue its decision according to the rules and procedures identified in the Bylaws. Such decision is appealable before the Grievance Dewan according to its Act. The amounts collected from such



penalties shall be delivered to the Commission and shall be considered a part of its revenues.



Chapter Eleven

Final Rules

Article Thirty-nine:

The Commission's decisions can be appealed to the Minister. If the Commission's decision is upheld by the Minister, the concerned party has the right to appeal to the Grievance Dewan according to its Act.

Article Forty:

The Bylaws shall be issued by a decree from the Minister based on the recommendation of the Commission Board.

Article Forty-one:

1. This Act shall be published in the official Gazette and shall be effective after 180 days from its date of publication . This Act shall replace the Telegraph Regulation issued by the Royal Order No. 8792 on 12.9.1356 H, and its amendments, and the Acts for Wireless Equipment Usage issued by the Royal Decree No. 49 on 30.10.1382H, and its amendments, and the Telephone Utility Regulation issued by the Royal Decree No. M/16 on 16.3.1398H, this Act also shall cancel the Automatic Telephone Rate Chart issued by the Council of Ministers' decree No. 517 on 21.4.1393H, and the Telex Services Organization and Rate Chart issued by the Council of Ministers' decree No. 123 on 24.8.1416H. Also this Act shall supersede all Acts which are in contradiction with it.
2. As an exception from Clause "1" of this Article, the current Regulations and the other Regulatory Decrees shall continue to be operative insofar as they do not contradict with this Act until its Implementation Bylaws are issued within a maximum period of 6 months from the effective date of this Act.