Electronic Transactions Act, 2008 Act 772

ARRANGEMENT OF SECTIONS

Object and scope of the Act

Section

Electronic transactions

Electronic government services

Certifying Agency

Consumer protection

Protected computers and critical database

THE SEVEN HUNDRED AND SEVENTY-SECOND

ACT

OF THE PARLIAMENT OF THE REPUBLIC OF GHANA
ENTITLED

ELECTRONIC TRANSACTIONS ACT, 2008

AN ACT to provide for the regulation of electronic communications and related transactions and to provide for connected purposes.

DATE OF ASSENT: *18th December, 2008.*

ENACTED by the President and Parliament:

Object of the Act

Object of the Act

1. (1) The object of this Act is to provide for and facilitate electronic communications and related transactions in the public interest, and to

(a) remove and prevent barriers to electronic communications and transactions;

(b) promote legal certainty and confidence in electronic communications and transactions;

(c) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;

(d) develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;

(e) promote the development of electronic transaction services responsive to the needs of consumers;

(f) ensure that, in relation to the provision of electronic transactions services, the special needs of vulnerable groups and communities and persons with disabilities are duly taken into account;

(g) ensure compliance with accepted international technical standards in the provision and development of electronic communications and transactions;

(h) ensure efficient use and management of the country domain name space; and

(i) ensure that the interest and image of the Republic are not compromised through the use of electronic communications.

Application

2. This Act applies to electronic transactions and electronic records of every type.

Scope of Act

3. (1) This Act shall not be interpreted so as to exclude statute law or the principles of the common law being applied to, recognising or accommodating electronic transactions, electronic records or any other matter provided for in this Act.

(2) Unless otherwise provided, this Act shall not be construed as

(a) requiring a person to generate, communicate, produce, process, send, receive, record, retain, store or display information, document or signature by or in electronic form; or

(b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept electronic records.

(3) This Act does not limit the operation of law that expressly authorises, prohibits or regulates the use of electronic records and any legal requirement law for information to be posted, displayed or transmitted in a specified manner.

Exclusion

4. This Act does not apply to:

(a) a negotiable instrument as defined in the Bill of Exchange Act, 1961 (Act 55);

(b) the grant of a power-of-attorney under the Powers of Attorney

Act, 1998 (Act 549);

(c) a trust as defined in the Trustees Incorporation Act, 1962 (Act 106);

(d) a will as defined in the Wills Act, 1971 (Act 360);

(e) a contract for the sale or conveyance of immovable property or any interest in the immovable property;

(f) bills of lading;

(g) documents required for the registration of a company, Partnership or sole proprietorships;

(h) the swearing of affidavits or statutory declarations before a Commissioner for Oaths or Notary Public; and

(i) any class of documents or transactions that may be notified by *Gazette.*

Electronic transactions

Recognition of electronic message

5. Except as provided in this Act, where a law provides that information or any other matter shall be in writing, typewritten or in printed form, the requirement shall be deemed to have been satisfied if the information or matter is

(a) rendered or made available in an electronic form,

(b) accessible, and

(c) capable of being retained for a subsequent reference

despite the contrary intention in the law.

Original writing

6. (1) Where a law requires information to be presented or retained in its original form, the requirement shall be deemed to have been satisfied by an electronic record if

(a) there is reliable assurance of the integrity of the electronic record, and

(b) the electronic record is capable of being displayed to the person to whom it is to be presented.

(2) The criteria to assess integrity shall be whether the information has remained complete and unaltered and the information shall be assessed taking into consideration the relevant circumstances for which the information was generated to determine the standard of reliability.

Admissibility and evidential weight of electronic records

7. (1) The admissibility of an electronic record shall not be denied as evidence in legal proceedings except as provided in this Act.

(2) In assessing the evidential weight of an electronic record the Court shall have regard to

(a) the reliability of the manner in which the electronic record was generated, displayed, stored or communicated,

(b) the reliability of the manner in which the integrity of the information was maintained,

(c) the manner in which its originator was identified, and

(d) any other facts that the Court may consider relevant.

Retention of electronic records

8. (1) Where a law requires that a document, record or information shall be retained, that requirement is deemed to have been met if the document, record or information is held in electronic form and

(a) is accessible,

(b) is capable of retention for subsequent reference,

(c) is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received, and

(d) is retained to enable the identification of the origin and destination of the electronic record and the date and time when it was sent or received.

(2) The document, record or information shall be kept in electronic form for at least six years.

(3) An obligation to retain a document, record or information does not extend to information which is only to enable the message to be sent or received.

Secure electronic record

9. (1) Where a security procedure has been applied to an electronic record at a specific point in time, the record is deemed to be a secure electronic record during the period when the security procedure was applied.

(2) An unauthorised alteration of the security procedure renders the record invalid.

(3) An alteration is unauthorised if it is done by a person without the lawful authority of the person who originally applied the security procedure.

Digital signature

10. (1) Where a law requires the signature of a person, that requirement is deemed to be satisfied in relation to an electronic record if a digital signature is used.

(2) A digital signature is deemed to be authentic if

(a) the means of creating the digital signature is, within the context in which it is used, linked to the signatory and not to another person,

(b) the means of creating the digital signature was, at the time of signing, under the control of the signatory and not another person without duress or undue influence , and

(c) an alteration to the digital signature, made after the time of signing, is detectable.

(3) Subsection (2) does not limit the right of a person

(a) to prove the authenticity of a digital signature in any other way, or

(b) to adduce evidence in respect of the non-authenticity of a digital signature.

Equal treatment of digital signatures

11. Except as provided in this Act, the provisions of this Act do not exclude, restrict, or deprive of legal effect, any method of creating a digital signature which

(a) satisfies the requirements of this Act,

(b) meets the requirements of other statutory provision, or

(c) is provided for under a contract.

Signing of an electronic record

12. A person may sign an electronic record by affixing a personal digital signature or using any other recognized, secure and verifiable mode of signing agreed by the parties or recognized by the industry to be safe, reliable and acceptable.

Conduct of a person relying on a digital signature

13. A person who relies on a digital signature shall bear the legal consequences of failure to

(a) take reasonable steps to verify the authenticity of a digital signature, or

(b) take reasonable steps where a digital signature is supported by a certificate, to

(i) verify the validity of the certificate, or

(ii) observe any limitation with respect to the certificate.

Recognition of digital certificates and digital signatures

14. (1) Unless otherwise prescribed by law, a person may determine the digital signature, certificate or authentication the person will use.

(2) The Minister may recognise a digital signature, certificate or authentication of a foreign information security service provider for use by a public servant by notice published in the *Gazette.*

Notarisation, acknowledgement and certification

15. (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is deemed to be satisfied if the electronic signature of the person authorised to perform those acts is affixed to an electronic record.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or in another physical form, that requirement is deemed to be satisfied if an electronic copy of the document is certified to be a true copy by using the electronic signature of the certifying person.

Other requirements

16. (1) A requirement in law for multiple copies of a document to be submitted to a single addressee at the same time, is satisfied by the submission of a single electronic record that is capable of being reproduced by the addressee.

(2) Where a corporate seal is required to be affixed to a document, that requirement is deemed to be satisfied if the electronic signature of the corporate body is affixed to the electronic record in accordance with the provisions relating to the use of the corporate seal.

Automated transactions

17. (1) An automated transaction is valid even if an electronic agent

is involved at any stage of its formation.

(2) A party interacting with an electronic agent to make an agreement is not bound by the terms of the agreement unless the terms were capable at first of being accessed by the party prior to the formation of the contract.

(3) An electronic contract is not valid where an individual interacts directly with the electronic agent and has made a material error during the creation of an electronic record and

(a) the electronic agent did not provide that person with an easy opportunity to prevent or correct the error,

(b) that person notifies the party creating the electronic record of the error as soon as practicable after noticing it,

(c) that person takes reasonable steps to return to the previous situation, and

(d) that person has not used or received material benefit or value from performance received from the other person.

Despatch of electronic record

18. Unless otherwise agreed between the originator and the addressee, the despatch of an electronic record occurs when it enters an information processing system outside the control of the originator or the agent of the originator.

Receipt of electronic record

19. The time of receipt of an electronic record shall be determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs at the time when the electronic record enters the designated information system, or

(b) if the addressee has not designated an information system, receipt occurs when the electronic record enters an information system of the addressee through which the addressee retrieves the electronic record.

(2) An electronic record is deemed to be despatched at the originator's registered place of business and is deemed to be received at the regis-

tered place where the addressee has its place of business unless otherwise agreed by the originator and the addressee.

Expression of intent or other statement

20. An expression of intent or other electronic representation of an electronic record between the originator and the addressee of an electronic record is admissible in circumstances where the intent or other electronic representation is relevant in law.

Attribution of electronic records to originator

21. (1) An electronic record is considered to be that of the originator if it was sent by

(a) the originator personally,

(b) a person who has authority to act on behalf of the originator in respect of that electronic record, or

(c) an information system programmed by or on behalf of the originator to operate automatically, unless it is proved that the information system did not properly execute the programme.

(2) An addressee is entitled to regard an electronic record as being that of the originator and to act on that assumption, if

(a) the addressee properly applied a procedure previously agreed with the originator in order to ascertain whether the electronic record was that of the originator, or

(b) the electronic record received by the addressee resulted from the actions of a person whose relationship with the originator or with an agent of the originator enabled that person to gain access to a method used by the originator to identify an electronic record as the originator's own.

(3) Where a procedure has not been agreed by both parties to ascertain the originator, the person who appears to be the originator shall be presumed to be the originator.

(4) The presumption in subsection (3) does not apply where:

(a) the addressee has received notice from the originator that the electronic record was issued without the knowledge or consent of the originator;

(b) the addressee knew or should reasonably have known, or used

any agreed procedure to know that the electronic record was not that of the originator and that the person who sent the electronic record did not have the authority of the originator to issue or send the electronic record; or

(c) the addressee knew or should reasonably have known, that the transmission resulted in an error in the electronic record as received.

Acknowledgement of receipt of electronic record

22. (1) An acknowledgement of receipt may be given through

(a) a communication by the addressee, whether automated or otherwise, or

(b) any conduct of the addressee to indicate to the originator that the electronic record has been received.

(2) An acknowledgement of receipt is not necessary to give legal effect to a message unless otherwise agreed by the parties.

Formation and validity of agreements

23. An agreement is valid even if it was concluded partly or in whole through an electronic medium.

Variation by agreement between parties

24. Sections 5 to 23 only apply if the parties involved in generating, sending, receiving, storing or otherwise processing electronic records have not agreed on the issues provided for by these sections.

Electronic government services

Acceptance of electronic filing and issuing of documents

25. A public body shall take steps or enter into arrangements to ensure that its functions are carried out, delivered or accessed electronically or online.

Public agency and electronic records

26. (1) A public agency that, pursuant to any law accepts the filing of documents, requires that documents be created or retained, issues a permit, licence or approval or provides for a payment in accordance with law, may

(a) accept the filing of a document, or the creation or retention of documents in the form of an electronic record,

(b) issue the permit, licence or approval in the form of an electronic record, or

(c) make or receive payment in electronic form or by electronic

means.

(2) Any public agency may specify by notice in the *Gazette:*

(a) the manner and format in which the electronic records shall be filed, created, retained or issued;

(b) the type of electronic signature required where the electronic record has to be signed;

(c) the manner and format in which an electronic signature shall be attached to, incorporated in or otherwise associated with the electronic record;

(d) the identity or criteria required of an authentication service provider used by the person filing the electronic record or the public agency may designate an authentication service provider as a preferred authentication service provider;

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(f) any other requirements for electronic records or payments.

Publication in electronic format

27. (1) Where a law requires publication in the *Gazette* the requirement is deemed to have been satisfied if published in electronic format referred to as an *E-Gazette.*

(2) The date of publication is deemed to be the date of first publication in the *Gazette.*

Certifying Agency

Prohibited acts

28. A person shall not sell or provide encryption or authentication service contrary to the provisions of this Act.

Provision of authentication encryption services

29. An encryption or an authentication service or product is deemed to have been provided in the country if it is made available:

(a) from premises within the country;

(b) from a body incorporated in the country;

(c) to a person who is present or operating from any system in the country when that person makes use of the service or product; or

(d) from a Ghanaian associated or related domain name or website.

Certifying Agency

30. (1) The National Information Technology Agency established under National Information Technology Agency Act 2008 (Ac 771) shall facilitate the establishment of the Certifying Agency under this Act.

(2) The Certifying Agency shall maintain a website and provide information at the website in accordance with this Act.

Functions of the Certifying Agency

31. The functions of the Agency are to:

(a) issue licences for encryption and authentication service;

(b) monitor the conduct, system and operation of encryption and authentication service providers to ensure compliance with conditions of the licence, and the provisions of this Act;

(c) suspend a licence of a licence holder;

(d) revoke a licence of a licence holder; and

(e) appoint an independent auditing firm to conduct periodic audits of a licence holder to ensure compliance with conditions of the licence and this Act.

Revocation or suspension of licence

32. (1) The Agency may suspend or revoke a licence if it is satisfied that the authentication service provider has failed or ceased to meet any of the requirements, conditions or restrictions subject to which the licence was granted or recognition was given.

(2) The Agency shall not suspend or revoke a licence unless it has

(a) notified the licence holder in writing of its intention to do so,

(b) given a description of the alleged breach, and

(c) afforded the licensed holder the opportunity to

(i) respond to the allegations in writing, and

(ii) remedy the alleged breach.

(3) The Agency may suspend a licence with immediate effect for a period not exceeding ninety days pending implementation of the procedures required to remedy the breach where there is the likelihood of irreparable harm to consumers or third parties involved in an electronic transaction.

(4) A licence holder may surrender the licence to the Agency subject to the provisions of the licence and third party rights.

(5) The Agency shall publish the suspension or revocation of a licence in the *Gazette.*

Surrender of licence

33. (1) A licensee with a suspended or revoked licence shall surrender the licence to the Agency within twenty-four hours of receipt of notice of the suspension or revocation of its licence.

(2) Where a licensee fails to surrender the licence, each director of the licensee commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units for each day that the licence is not surrendered or to a term of imprisonment of not more than two years or to both.

Recognition of foreign certifying authorities

34. (1) Subject to the conditions and restrictions that may be specified by law, the Agency may, by notification in the *Gazette,* recognise a foreign entity as a certifying agency.

(2) Where a foreign entity is recognized, as a certifying agency, service and products issued by a person pursuant to the directives of that foreign certifying agency are valid.

(3) The Agency by notification in the *Gazette* may revoke the recognition if it is satisfied that a foreign certifying agency has contravened any of the conditions and restrictions subject to which it was granted recognition.

Repository of digital signatures

35. (1) The Agency shall be the repository of Digital Signature Certificates issued under this Act.

(2) The Agency shall

(a) make use of hardware, software and procedures that are secure from intrusion and misuse, and

(b) observe other standards that may be prescribed, to ensure that the secrecy and security of digital signatures are assured.

(3) The Agency shall maintain a computerized data base of the public keys to make them verifiable by a member of the public.

Register of licence holders

36. (1) The Agency shall establish and maintain a register of licence holders.

(2) The Agency shall record the following particulars in respect of each licence holder

(a) the name and address of the licence holder,

(b) a description of the type of service or product provided,

(c) other particulars that may be prescribed to identify and locate

the license holder or its products or services,

(d) licensed encryption and authentication products or services under this Act,

(e) licensed encryption and authentication products and services recognised under this Act,

(f) suspended and revoked licences or recognition, and

(g) any other information that may be prescribed or may be deemed appropriate by the Agency.

(3) The Agency shall provide notice of the suspension or revocation at its website.

(4) The Agency shall publish the list of licence holders, revoked or suspended licences in electronic and other media, subject to the rules relating to confidentiality.

(5) A licence holder shall not be required to disclose confidential information or trade secrets in respect of its products or services.

Restrictions on disclosure of information

37. Subject to the provisions of the Constitution, a person may make disclosure of information under this Act

(a) to a law enforcement agency,

(b) for criminal or civil proceedings,

(c) to government agencies responsible for safety and security on official request, and

(d) to a third party enquiry for confirmation of a licence or representations made by a licence holder.

Application for licence

38. (1) A licence shall not be issued or granted by the Agency to an individual.

(2) Each application for the issue of a licence shall be in the prescribed form.

(3) Each application for a licence shall be accompanied with,

(a) a certificate of incorporation,

(b) a statement including the procedures with respect to the identification of the applicant.

(c) payment of a non-refundable application fee, and

(d) other prescribed documents.

(4) The Agency shall take the following factors into account in considering an application:

(a) the financial and human resources, including the assets of an applicant;

(b) the quality of the applicants hardware and software systems;

(c) procedures for processing products or services;

(d) the availability of information to third parties relying on the authentication product or service;

(e) the regularity and extent of audits by an independent body; and

(f) any other relevant factor which may be prescribed or which the Agency may consider necessary.

(5) A licence is valid for the period and on the terms and conditions that may be determined by the Agency.

Grant of licence

39. (1) The Agency shall not grant a licence under this Act unless the Agency is satisfied that a security procedure related to or issued by an applicant,

(a) is uniquely linked to the user,

(b) is capable of identifying that user,

(c) is created using means that can be maintained under the sole control of that user, and

(d) will be linked to the electronic record to which it relates so that any subsequent change of the electronic record is detectable.

(2) The Agency may, prior to licensing any authentication products or services, stipulate:

(a) the technical and other requirements to be met by certificates issued by the licence holder;

(b) the requirements for issuing certificates;

(c) the requirements for certification practice statements;

(d) the responsibilities of the certification service provider;

(e) the liability of the certification service provider;

(f) the records to be kept and the manner in which and length of time for which they must be kept;

(g) requirements concerning certificate suspension and revocation procedures;

(h) requirements as to notification procedures relating to certificate suspension and revocation; and

(i) other conditions or restrictions that the Agency may consider necessary.

(3) A licence is not transferable.

Display of licence

40. A licensee shall display its licence conspicuously on the premises of its principal place of business.

Duties of licensed entities

41. A licensee shall ensure that each person employed or engaged by it complies with the provisions of this Act, Regulations made under this Act and the licence conditions.

Renewal of licence

42. An application for renewal of a licence shall be

(a) in the form, and

(b) accompanied with the fees prescribed and shall be paid in full before the issue of a licence.

Procedure for grant or rejection of renewal of licence

43. (1) The Agency may grant or reject the application for the renewal after considering the documents accompanying the application for renewal and other factors considered necessary.

(2) The Agency shall provide reasons for the rejection of the application in writing to the applicant.

Notification of adverse event

44. The Agency shall

(a) use reasonable efforts to notify any person who is likely to be affected by the occurrence of an adverse event, or

(b) deal with the event or situation in accordance with the procedure specified in its certification practice statement

where in the opinion of the Agency an event has occurred or a situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a licence was granted.

Procedures to be followed by licensed person

45. A licensed person shall

(a) make use of hardware, software and procedures that are secure from intrusion and misuse,

(b) provide such level of reliability in its services which are reasonably suited to the performance of the intended functions,

(c) adhere to security procedures to ensure that the secrecy and privacy of the product or service are assured, and
(d) adhere to such security procedures and observe such other standards as may be prescribed.

Consumer protection

Scope of application

46. Sections 47 to 54 apply only to electronic transactions.

Information to be provided

47. (1) The supplier offering goods or services for sale, hire or exchange in an electronic transaction shall make available to the consumer on the electronic platform where the goods or services are offered the following information related to the supplier:

(a) full name and legal status;
(b) physical address and telephone number;
(c) website address and e-mail address;
(d) membership of any self-regulatory or related bodies and the contact details of the body;
(e) a code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;
(f) the registration number, the names of office bearers and the place of registration of a legal person;
(g) sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;
(h) the full price of the goods or services, including transport costs, taxes and any other fees or costs;
(i) the manner of payment;
(j) terms of agreement including guarantees that will apply to the transaction and how these terms may be accessed, stored and reproduced electronically by consumers;
(k) the time within which the goods will be despatched or delivered or within which the services will be rendered;
(l) the manner and period within which consumers can access and maintain a full record of the transaction;
(m) the return, exchange and refund policy;

(n) the alternative dispute resolution code to which that supplier subscribes and access to the code by the consumer;

(o) the security procedures and privacy policy of that supplier as regards payment, payment information and personal information;

(p) the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently where appropriate; and

(q) the rights of consumers as provided for in this section.

(2) The supplier shall provide a consumer with an opportunity to

(a) read, store and reproduce the contract terms and general conditions,

(b) identify and correct handling errors, and

(c) withdraw from the transaction before concluding a contract.

(3) If a supplier fails to comply with the provisions of this section, the consumer may cancel the contract within fourteen days of receipt of the goods or services under the transaction.

(4) If a transaction is cancelled as a result of the failure of the supplier to comply with the provisions of this section

(a) the consumer shall return the goods received, or where applicable, cease using the services performed, and

(b) the supplier shall refund payments made by the consumer within thirty days.

(5) The supplier shall utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.

(6) The supplier is liable for damage suffered by a consumer due to failure by the supplier to apply a secure payment system.

Performance

48. (1) The supplier shall execute the order within fourteen days after the day on which the supplier receives the order, unless the parties have agreed otherwise.

(2) Where a supplier fails to execute the order within the fourteen days or within the agreed period, the contract is voidable.

(3) If a supplier is unable to perform on the grounds that the goods

or services ordered are unavailable, the supplier shall immediately notify the consumer of this fact and refund any payment within seven days after the date of notification.

Grace period

49. (1) A consumer is entitled to cancel a transaction and any related credit agreement for the supply

(a) of goods within fourteen days after the date of the receipt of the goods, or

(b) of services within seven days after the date of the conclusion of the agreement,

without reason and without penalty.

(2) The only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) This section shall not be construed to limit the rights of a consumer provided for in any other law.

(4) This section does not apply to an electronic transaction:

(a) for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;

(b) by way of an auction;

(c) for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;

(d) for services which began with the consumer's consent before the end of the seven-day grace period;

(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(f) where the goods

(i) are made to the consumer's specification,

(ii) by reason of their nature cannot be returned, or

(iii) are perishable;

(g) where audio or video recordings or computer software were unsealed by the consumer;

(h) for the sale of newspapers, periodicals, magazines and books;

(i) for the provision of gaming and lottery services; or

(j) for the provision of accommodation, transport, catering or leisure services where the supplier has commenced the provision of these services on a specific date or within a specific period.

Unsolicited goods, services or communications

50. (1) Except in the case of a notice sent by an electronic communications provider to a customer in relation to the service, a person shall not send unsolicited electronic communications to a consumer without obtaining the prior consent of the consumer.

(2) A person who sends electronic commercial communication to a consumer shall provide the consumer

(a) with the option to cancel the subscription to the mailing list of that person, and

(b) with the identifying particulars of the source from which that person obtained the consumer's personal information at the request of the consumer.

(3) An agreement shall not be deemed to have been concluded where a consumer fails to respond to an unsolicited communication; and the consumer is entitled to recover the costs associated with the cancellation of unsolicited communication.

(4) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

(5) A person who sends unsolicited commercial communications to another person or who continues to send unsolicited commercial communications after cancellation of the subscription commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

Liability for misuse of electronic payment medium

51. (1) A holder of an electronic payment medium shall not, unless acting in collusion with another person, be liable to the issuer for loss arising from use of the medium by a person who is not acting or being treated as acting as the agent of the holder.

(2) Subsection (1) does not prevent

(a) the holder of the electronic payment medium from being made liable for loss to the issuer arising from use of the medium by another person during a period beginning when the medium ceases to be in the possession of an authorised person and ending when the medium is once more in the possession of an authorised person, or

(b) the holder from being made liable to any extent for loss to the issuer from use of the medium by a person who acquired possession of it with the holder's consent.

(3) Subsections (2) does not apply to the use of the electronic payment medium after the issuer has been given notice of loss and does not apply unless the issuer provides the holder with particulars of the name, address and telephone number of a person stated to be the person to whom notice is to be given.

(4) The notice takes effect when received, but where it is given orally, shall be confirmed in writing within fourteen clear days.

(5) A sum paid by the holder for the issue of the electronic payment medium is treated as paid towards satisfaction of liability under this section to the extent that it has not been previously offset by use made of the medium.

(6) The holder or a person authorised by the holder to use the electronic payment medium is an authorised person for the purpose of subsection (2).

Electronic payment medium lists prohibited

52. (1) A financial institution shall not

(a) make available,

(b) lend, or

(c) sell

any list or portion of a list of holders of an electronic payment medium and their addresses and account numbers to any person without the prior written consent of the holders except by order of a Court.

(2) A financial institution may make available to another financial institution information about an electronic payment medium holder's credit rating without the holder's prior written consent if written notice

of the disclosure is given to the holder within seven days subject to any law regulating credit rating institutions.

(3) A financial institution which contravenes subsection (1) commits an offence and each director and officer of the institution who fails to ensure compliance with this Act is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or imprisonment for a term of not more than five years or to both.

Applicability of foreign law

53. Despite a provision of an agreement to the contrary, the supply of goods pursuant to a contract to consumers in this country is subject to the provisions of this Act.

Non-exclusion

54. A provision in an agreement which excludes consumer rights provided for in this Act is void.

Protected computers and critical database

Protected computer

55. (1) The Minister may declare that a computer, computer system or computer network is a protected system by notification in the *Gazette*.

(2) The Minister may authorise access to a protected system by or in writing.

(3) Until the Minister by *Gazette* publication declares a computer, computer system or computer network to be a protected system, the computer , computer system or computer network shall be treated as a "protected computer" if the computer, program or electronic record is used directly in connection with or for

(a) the security, defence or international relations of the country;

(b) the existence or identity of a confidential source of information related to the enforcement of criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure;

(d) the protection of public safety and public health, including systems related to essential emergency services;

(e) foreign commerce or communication affecting a citizen of Ghana or business in which a citizen of Ghana or the Government has an interest; or

(f) the legislative, executive or judicial service, the public services and security agencies.

(4) A person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or imprisonment for a term of not more than ten years or to both.

Identification of critical electronic record and critical databases

56. The Minister may by notice in the *Gazette*

(a) declare certain classes of information which are of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical electronic records for the purpose of this Act, and

(b) establish a procedure to be followed in the identification of critical databases for the purposes of this Act.

Scope of critical database protection

57. The Minister may declare certain classes of information relating to national security or the economic or social wellbeing of the public to be critical electronic record for the purposes of sections 58 to 62.

Registration of critical databases

58. (1) The Minister may by notice in the *Gazette* determine

(a) requirements for the registration of a critical database,

(b) procedures for the registration of a critical database, and

(c) any other matter relating to registration.

(2) Registration of a critical database means recording the following information:

(a) the full name, address and contact details of the critical database administrator;

(b) the location of the critical database, including the locations of the component parts where a critical database is not stored at a single location; and

(c) a general description of the categories or types of information stored in the critical database.

Management of critical databases

59. (1) The Minister shall prescribe minimum standards for prohibitions in respect of

(a) the general management of a critical database,

it considers necessary for the protection of national security.

Domain name registry

Establishment of Registry

63. (1) There is established by this Act a Domain Name Registry.

(2) The Registry is a body corporate with perpetual succession and a common seal and may sue and be sued in its corporate name.

(3) The Registry may be converted into a company limited by guarantee on the same terms and conditions as provided under this Act.

(4) The Registry is a non-profit making entity.

Functions of the Registry

64. (1) The Registry is responsible for the country domain name space from a date to be determined by the Minister by notice in the *Gazette* and shall

(a) administer and manage the country domain name space;

(b) comply with international best practice in the administration of the .gh domain name space;

(c) license and regulate registries;

(d) license and regulate registrars for the respective registries; and

(e) publish guidelines on

(i) the general administration and management of the .gh domain name space,

(ii) the requirements and procedures for domain name registration, and

(iii) the maintenance of and public access to a repository,

with due regard to the policy directives which the Minister may give from time to time by notice in the *Gazette*.

(2) After the assumption of responsibility for the country domain space, a person shall not do anything or operate the country domain name or any domain name associated with the country except as provided under this Act.

(3) A person who contravenes this section commits an offence and is liable on summary conviction to a fine of not more than five hundred penalty units or to a term of imprisonment of not more than three years or to both.

Duties of the Registry

65. (1) The Registry shall enhance public awareness on the economic

(b) access to, transfer and control of a critical database,

(c) infrastructural or procedural rules and requirements to secure the integrity and authenticity of a critical electronic record,

(d) procedures and technological methods to be used in the storage or archiving of a critical database,

(e) accident recovery plans in the event of loss of critical data bases or parts of the database,

(f) the security of the databases,

(g) the physical safety of a person in control of the critical database, and

(h) any other matter required for the adequate protection, management and control of a critical database.

(2) This Act shall not be construed to limit the right of a public body to perform an authorised function in terms of any other law.

Restrictions on disclosure of information

60. (1) Information contained in the register of a critical database shall not be disclosed to another person other than to employees of the Agency who are responsible for the keeping of the register.

(2) The Agency is at liberty to disclose information to

(a) a law enforcement agency, and

(b) a Ministry, Department or Agency.

(3) Nothing in this law shall preclude the Agency from pleading in proceedings relating to information held in its custody or records that production or disclosure of a matter may be prejudicial to the security of the State or injurious to the public interest in accordance with article 135 of Constitution.

Right of inspection

61. The Minister may cause audits to be carried out by a critical database administrator to evaluate compliance with the provisions of this Act.

Non-compliance with Act

62. (1) The Minister on receipt of the audit report shall consider,

(a) any action recommended to remedy the non-compliance, and

(b) the period within which the remedial action shall be performed.

(2) The Minister shall report the recommendation to the National Security Council and the Council may take action or give directions that

and commercial benefits of domain name registration.

(2) The Registry

(a) may conduct investigations related to its functions that it considers necessary,

(b) shall conduct research into and keep abreast with developments in the country and elsewhere on the domain name system,

(c) shall continually survey and evaluate the extent to which the .gh domain name space meets the needs of the citizens, and

(d) may issue information on the registration of domain names in the country.

(3) The Registry may, and shall when requested by the Minister, make recommendations to the Minister in relation to policy concerned with the .gh domain name space.

(4) The Registry shall continually evaluate the effectiveness of this Act and action taken towards the management of the .gh domain name space.

(5) The Registry may

(a) liaise, consult and co-operate with any person or other Registry, and

(b) appoint experts and other consultants on conditions that the Registry may determine.

Licensing of registrars and registries

66. (1) A person shall not update a repository or administer a second level country domain name unless the person is licensed to do so by the Registry.

(2) An application to be licensed as a registrar or registry shall be made in the prescribed manner and subject to the prescribed fees.

(3) The Registry shall apply the prescribed conditions and criteria when evaluating an application.

Governing body of the Domain Name Registry

67. (1) The governing body of the Registry is a Board consisting of

(a) one person nominated by Council for Scientific and Industrial Research,

(b) one person nominated by the Minister of the Interior from the law enforcement agencies,

(c) one person nominated by the public universities,

(d) one person nominated by the private universities;

(e) the Executive Director of the Board,
(f) two persons nominated by the Industry Forum established under section 88 of this Act, and
(g) two other persons with interest in the development of the Ghana domain name one of whom is a woman nominated by the Minister.

(2) The members of the Board shall be appointed by the President in accordance with article 70 of the Constitution.

(3) The President shall appoint one of the members to be the chairperson.

(4) The Board shall ensure the proper and effective performance of the functions of the Registry.

Tenure of office of members

68. (1) A member of the Board shall hold office for a period not exceeding four years and is eligible for re-appointment but a member shall not be appointed for more than two terms in succession.

(2) Where a member of the Board, resigns, dies, is removed from office or is for a reasonable cause unable to act as a member, the minister shall notify the President of the vacancy and the President shall, acting on the advice of the nominating authority and in consultation with the Council of State appoint another person to hold office for the unexpired portion of the member's term of office.

(3) A member of the Board, who is absent from three consecutive meetings of the Board without reasonable cause ceases to be a member of the Board.

(2) A member of the Board, may at any time resign from office in writing addressed to the President through the Minister.

(5) The President may by letter addressed to a member revoke the appointment of that member.

Meetings of the Board

69. (1) The Board shall meet at least once every two months for the despatch of business at the times and in the places determined by the chairperson.

(2) The chairperson shall at the request in writing of not less than one-third of the membership of the Board convene an extraordinary meeting of the Board at the place and time determined by the chairperson.

(3) The quorum at a meeting of the Board is four members.

(4) The chairperson shall preside at meetings of the Board and in the absence of the chairperson a member of the Board elected by the members present from among their number shall preside.

(5) Matters before the Board shall be decided by a majority of the members present and voting and in the event of an equality of votes, the person presiding shall have a casting vote.

(6) The Board may co-opt a person to attend a Board meeting but that person shall not vote on a matter for decision at the meeting.

(7) The proceedings of the Board shall not be invalidated because of a vacancy among the members or a defect in the appointment or qualification of a member.

(8) Subject to this section, the Board may determine the procedure for its meetings.

Disclosure of interest

70. (1) A member of the Board who has an interest in a matter for consideration by the Board shall disclose in writing the nature of that interest and is disqualified from participating in the deliberations of the Board in respect of that matter.

(2) A member who contravenes subsection (1) ceases to be a member.

Appointment of committees

71. (1) The Board may appoint committees consisting of members of the Board or non-members or both to perform a function.

(2) A committee of the Board may be chaired by a member of the Board.

Dispute Resolution Committee

72. (1) Without limiting section 71 the Board shall establish a Dispute Resolution Committee the composition of which shall be determined by the Board.

(2) The Committee shall expeditiously hear and inquire into and investigate any matter which is brought before it.

(3) The Committee shall determine the periods that are reasonably necessary for the fair and adequate presentation of the matter by the respective parties and the Agency may require those matters to be presented

within the periods.

(4) The Committee may require evidence or arguments to be presented in writing and may decide the matters upon which it will hear oral evidence or written arguments.

(5) Each party to a matter is entitled to appear at the hearing and may be represented by a lawyer or any other person.

Powers of the Dispute Resolution Committee

73. (1) The Dispute Resolution Committee may

(a) issue summons to compel the attendance of witnesses under the hand of the Secretary;

(b) examine witnesses on oath, affirmation or otherwise;

(c) compel the production of documents;

(d) cite a person for trial at the High Court for contempt;

(e) to make a declaration setting out the rights and obligations of the parties to the dispute;

(f) make provisional or interim orders or awards that relate to the matter or part of it, or give directions in pursuance of the hearing;

(g) dismiss or refrain from hearing or determining a matter, in whole or in part, if it appears that the matter, or part of the matter, is trivial or vexatious or that further proceedings are not necessary or desirable in the public interest;

(h) in appropriate circumstances, order any party to pay the reasonable costs and expenses of another party, including the expenses of witnesses and fees of lawyers, in bringing the matter before the Agency; and

(i) generally give directions and do what is necessary or expedient for the hearing and determination of the matter.

Allowances

74. Members of the Board and members of a committee of the Board shall be paid allowances approved by the Minister in consultation with the Minister responsible for Finance.

The Executive Director

75. (1) The President shall, in accordance with article 195 of the Constitution, appoint a Executive Director for the Registry.

(2) The Executive Director shall hold office on the terms and conditions specified in the letter of appointment.

Functions of the Executive Director

76. (1) The Executive Director is responsible for the day to day administration of the affairs of the Registry and is answerable to the Board in the performance of functions under this Act.

(2) The Executive Director shall perform any other functions determined by the Board.

(3) The Executive Director may delegate a function to an officer of the Registry but shall not be relieved from the ultimate responsibility for the performance of the delegated function.

Appointment of other staff

77. (1) The President shall in accordance with article 195 of the Constitution appoint other staff of the Registry that are necessary for the proper and effective performance of its functions.

(2) Other public officers may be transferred or seconded to the Registry or may otherwise give assistance to it.

(3) The Registry may engage the services of advisers and consultants on the recommendations of the Board.

Funds of the Registry

78. The funds of the Registry include

(a) moneys provided by Parliament,

(b) donations, grants and gifts,

(c) fees, and

(d) any other moneys that are approved by the Minister responsible for Finance.

Accounts and audit

79. (1) The Board shall keep books of account and proper records in relation to them in the form approved by the Auditor-General.

(2) The Board shall submit the accounts of the Registry to the Auditor-General for audit within three months after the end of the financial year.

(3) The Auditor-General shall, not later than three months after the receipt of the accounts, audit the accounts and forward a copy of the audit report to the Minister.

(4) The Internal Audit Agency Act, 2003 (Act 658) shall apply to this Act.

(5) The financial year of the Registry is the same as the financial year of the Government.

Annual report and other reports

80. (1) The Board shall within one month after the receipt of the audit report, submit an annual report to the Minister covering the activities and the operations of the Registry for the year to which the report relates.

(2) The annual report shall include the report of the Auditor-General.

(3) The Minister shall, within one month after the receipt of the annual report, submit the report to Parliament with a statement that the Minister considers necessary.

(4) The Board shall also submit to the Minister any other reports which the Minister may require in writing.

Resolution of disputes

81. (1) The Agency shall establish a dispute resolution process for the determination of the following disputes

(a) a dispute between or among different licence holders,

(b) a dispute between a licence holder and a consumer, and

(c) a dispute between the Domain Name Registry of Ghana and any licence holder or applicant for a licence.

(2) One or more parties to a dispute may refer the dispute to the Agency.

(3) The Agency may by legislative instrument make regulations on the manner and procedure for the resolution of disputes.

Appeal Tribunal

Establishment of the Information Communication Technology Tribunal

82. (1) There is established by this Act an appeal tribunal, known as the Information Communication Technology Tribunal referred to in this Act as "the Tribunal".

(2) The Tribunal shall be convened on an adhoc basis to consider an appeal

(a) against a decision or order made by the Agency,

(b) on a particular matter under a licence, and

(c) on a decision of the Dispute Resolution Committee.

Composition of the Tribunal

83. (1) The Tribunal consists of

(a) a chairperson who is either a retired Justice of the Superior Court or a lawyer of at least fifteen years standing who has experience in electronic communication law, policy and

regulatory matters or arbitration, and

(b) two other members with knowledge of or experience in the information communication technology related matters, industry, electronic engineering, law, economics, business or public administration.

(2) The members of the Tribunal shall be appointed by the Public Services Commission.

(3) The Public Services Commission shall also appoint a Registrar for the Tribunal for the smooth operations of the Tribunal.

(4) The Registrar and other staff are employees of the Agency.

(5) The expenses of the Tribunal shall be paid out of income derived by the Agency and shall be part of the annual budget of the Agency.

Rules of Procedure of Tribunal

84. The Board shall, propose rules of procedure for the Tribunal.

Appeals against decisions of the Agency or Dispute Resolution Committee

85. (1) A person affected by a decision of the Agency or the Dispute Resolution Committee may appeal against the decision by notice of appeal to the Tribunal in accordance with the rules of procedure of the Tribunal.

(2) The notice of appeal shall be sent within twenty-eight days after the date the decision is announced or the date of receipt of the decision that is being appealed against.

(3) The notice of appeal shall set out

(a) the decision appealed against,

(b) the provision under which the decision appealed against was taken, and

(c) the grounds of appeal.

(4) After the receipt of a notice of appeal, the Tribunal shall be convened within one month to consider the appeal.

Decision of Tribunal

86. (1) The Tribunal, after hearing the appeal, may

(a) quash the decision,

(b) allow the appeal in whole or in part,

(c) vary the decision of the Agency in any manner and subject to any conditions or limitations it thinks fit but shall not impose any condition or requirement beyond the powers of the Agency under the Act, or

(d) dismiss the appeal and confirm the decision of the Agency.

(2) The Tribunal may take into account a submission filed by any person in reaching a decision on an appeal brought before it.

(3) A decision of the Tribunal shall have the same effect as a judgment of the High Court.

Appeals against the decisions of the Tribunal

87. (1) A decision of the Tribunal may be the subject of an appeal.

(2) An appeal under this section

(a) lies to the Court of Appeal,

(b) shall relate only to a point of law arising from the decision of the Tribunal, and

(c) may be brought only by a party to the proceedings before the Tribunal.

(3) The appeal shall be filed in the Court of Appeal ninety days after the decision of the Tribunal and there shall be no extension of time.

Industry Forum

Establishment of Industry Forum

88. (1) There is hereby established an Industry Forum which shall be a platform to bring the industry together from time to time to discuss matters of common interest that relate to the industry.

(2) The Agency may designate an industry body to be the Forum by notifying that body in writing if the Agency is satisfied that

(a) the membership of the body is open to the relevant parties and is fully representative of the industry,

(b) the body is capable of performing as required under the relevant provisions of this Act, and

(c) the body has the administrative capacity to service the Forum.

(3) The body shall agree in writing to be the Forum, before being designated by the Agency.

(4) Despite the designation, each licensed entity under the Act is deemed to be a member of the Forum.

(5) The Agency may decide that an existing industry body that was previously designated under subsection (2) to be an Industry Forum is no longer an Industry Forum if satisfied that the body does not meet the requirements of this section any longer.

(6) A designation or withdrawal of designation under this section takes effect from the date specified by the Agency.

(7) Until the Agency designates a body, the Agency has the obliga-

tion to facilitate the meeting of the industry to perform the functions of the Forum.

(8) The Ministry and the Agency shall participate in the Forum as observers.

Industry code

89. (1) The Forum may prepare a voluntary industry code to deal with a matter provided for in this Act

(a) on its own initiative, or

(b) at the request of the Agency.

(2) The code shall not be effective until it is registered by the Agency.

(3) The Agency shall register a voluntary industry code if it is consistent with

(a) the objects of this Act,

(b) regulations, standards or guidelines made under this Act, and

(c) provisions of this Act which are relevant to the particular matter or activity.

(4) The Agency may refuse to register the code, if the Agency is not satisfied that there has been sufficient opportunity for public consultation in the development of the code by the Forum.

(5) The Agency shall notify the Forum in writing and provide the reasons for the refusal to register the code within thirty days after the refusal.

(6) Where the Agency does not register or refuses to register a voluntary industry code within a period of thirty days after the date that the voluntary industry code was submitted for registration, the Agency is deemed to have refused the registration of the voluntary industry code unless the Industry Forum receives a written notice of registration of the voluntary industry code after that period.

Liability of service providers and intermediaries

Mere conduit

90. (1) An intermediary or service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of electronic records through an information system under its control, as long as the intermediary or service provider

(a) does not initiate the transmission,

(b) does not select the addressee,

(c) performs the functions in an automatic, technical manner without selection of the electronic record, and

(d) does not modify the electronic record contained in the transmission.

(2) The acts of transmission, routing and provision of access include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place

(a) for the sole purpose of carrying out the transmission in the information system,

(b) in a manner that makes it ordinarily inaccessible to anyone other than an anticipated recipient, and

(c) for a period no longer than is reasonably necessary for the transmission.

Electronic record transmission

91. An intermediary or service provider who transmits an electronic record provided by a recipient of the service through an information system under its control is not liable for the automatic, intermediate and temporary storage of that electronic record, where the purpose of storing the electronic record is to make the onward transmission of the electronic record more efficient to other recipients of the service on their request, as long as the service provider

(a) does not modify the electronic record,

(b) complies with conditions on access to the electronic record,

(c) complies with rules regarding the updating of the electronic record, specified in a manner widely recognised and used by the industry,

(d) does not interfere with the lawful use of technology widely recognised and used by the industry to obtain information on the use of the electronic record, and

(e) removes or disables access to the electronic record it had stored upon receiving a take-down notice under this Act.

Hosting

92. (1) An intermediary or service provider who provides a service that consists of the storage of electronic records provided to a user of the service, is not liable for damages arising from information stored at the request of the recipient of the service, as long as the service provider

(a) does not have actual knowledge that the information or an activity relating to the information is infringing the rights of

a third party,

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the information is apparent or can be reasonably inferred, and

(c) upon receipt of a take-down notification under this Act, takes action expeditiously to remove or to disable access to the information.

(2) The limitations on liability established by this section do not apply to a service provider unless

(a) it has provided an address to receive notifications of infringement, or

(b) it has an agent for receipt of notification of infringement.

Information location tools

93. An intermediary or service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing electronic record or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the intermediary or service provider

(a) does not have actual knowledge that the electronic record or an activity relating to the electronic record is infringing the rights of that person or the State;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the electronic record is apparent or can be reasonably inferred;

(c) does not receive a financial benefit directly attributable to the infringing activity; and

(d) removes or disables access to the reference or link to the electronic record or activity within a reasonable time after being informed that the electronic record or the activity relating to the electronic record, fringes the rights of a person or the State.

Take-down notification

94. (1) A person who claims that an electronically published matter is illegal or unlawful shall notify the publisher.

(2) A notification of unlawful activity shall be in a permanent medium addressed by the complainant to the intermediary or service

provider or its designated agent and shall include

(a) the full names and address of the complainant,

(b) the written or electronic signature of the complainant,

(c) identification of the right that has allegedly been infringed

(d) identification of the material or activity that is claimed to be the subject of unlawful activity,

(e) the remedial action required to be taken by the intermediary or service provider in respect of the complaint, and

(f) telephonic and electronic contact details, if any, of the complainant.

(3) A person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable to pay a pecuniary penalty equivalent to five hundred penalty units.

(4) The intermediary or service provider is liable for wrongful takedown in response to a notification.

Monitoring and compliance

95. (1) An intermediary or service provider shall not be required to monitor an electronic record processed by means of a personal system in order to ascertain whether its processing would constitute or give rise to an offence or give rise to civil liability.

(2) Nothing in this section shall relieve an intermediary or service provider from

(a) an obligation to comply with an order or direction of a Court or other competent Agency, or

(b) any contractual obligation.

Limitations and prohibited acts

96. (1) Except as provided in this Act

(a) any person or entity that provides an electronic communication service to the public shall not knowingly divulge the contents of a communication while in electronic storage by that service to any person or entity, and

(b) a person or entity providing remote computing service to the public shall not knowingly divulge the contents of any communication which is carried or maintained on that service to any other person or entity

(i) on behalf of, and received by means of electronic

transmission from a subscriber or customer of the service; and

(ii) solely for the purpose of providing storage or computer processing services to the subscriber or customer,

if the provider is not authorised to access the contents of the communications to provide any service other than storage or computer processing.

(2) A person or entity may divulge the contents of a communication

(a) to an addressee or intended recipient of the communication or an agent of the addressee or intended recipient;

(b) as otherwise authorised by law;

(c) with the lawful consent of the originator, an addressee, intended recipient of the communication, or the subscriber in the case of remote computing service;

(d) to a person employed, authorised or whose facilities are used to forward the communication to its destination;

(e) as may be necessarily incident to the provision of the service or to the protection of the rights or property of the provider of that service; or

(f) to a law enforcement agency if the contents were inadvertently and unintentionally obtained by the service provider and appear to relate to the commission of a crime.

Savings

97. Sections 89 to 96 do not affect

(a) an obligation founded on an agreement,

(b) the obligation of a service provider acting as in that capacity under a licensing or other regulatory regime established by or under any law, and

(c) an obligation imposed by law or by a Court order to remove, block or deny access to an electronic record.

Cyber inspectors

Powers of law enforcement officers

98. (1) This provision is in addition to the powers of arrest, search and seizure of a law enforcement agency provided by law.

(2) A law enforcement agent may seize any computer, electronic record, program, information, document, or thing in executing a warrant under this Act if the law enforcement officer has reasonable grounds to

believe that an offence under this Act has been or is about to be committed.

Law enforcement officer and third party assistance

99. (1) A law enforcement officer executing a warrant may be accompanied by an authorised person and is entitled, with the assistance of that person, to

(a) have access to and inspect and check the operation of any computer to which this section applies;

(b) use or cause the computer to be used to search any programme or electronic record held in or available to the computer;

(c) have access to information, any code or technology which has the capability of retransforming or unscrambling an encrypted programme or electronic record held in or available to the computer into readable and comprehensible format or text to investigate an offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under sections 98 to 106; and

(d) make and take away a copy of any programme or electronic record held in the computer as specified in the search warrant and any other programme or electronic record held in that or any other computer which the law enforcement officer has reasonable grounds to believe is evidence of the commission of another offence.

(2) A law enforcement officer executing a warrant under this Act is entitled to require

(a) the person by whom or on whose behalf, the police officer has reasonable grounds to suspect, to produce a computer which is or has been used, or

(b) any person in charge of, or otherwise concerned with the operation of the computer,

to provide the officer or any authorised person with the reasonable technical and other assistance required for investigation or prosecution.

(3) A law enforcement officer executing a warrant under this Act is entitled to require a person in possession of decryption information to grant the law enforcement officer access to the decryption information necessary to decrypt an electronic record required to investigate an offence.

Preservation of evidence

100. (1) A provider of wire or electronic communication services or a remote computing service on the written request of a law enforcement agency, shall take the necessary steps to preserve records and other

evidence in its possession pending the issue of a Court order and shall take steps to ensure that the request by the law enforcement agency is not disclosed to third parties during the period.

(2) Where an order from the Court is not obtained and served for fourteen days after the re ceipt of the written request, the wire or electronic communication services, or remote computing service provider is not under any obligation to preserve the evidence.

Contents of electronic communications in electronic storage

101. (1) A Court may order the disclosure of the contents of an electronic communication that is in transit, held, maintained or has been in electronic storage in an electronic communications system by an electronic communication service provider.

(2) The Court shall not make an order unless it is satisfied that the disclosure is relevant and necessary for investigative purposes or is in the interest of national security.

Disclosure of electronic information

102. (1) Except as provided in this Act, a provider of an electronic communication service or remote computing service shall not disclose a record or other information pertaining to a subscriber to a customer of an electronic communication service to any person without the consent of the subscriber or customer.

(2) A provider of an electronic communication service or remote computing service shall disclose a record or other information related to a subscriber or customer to a law enforcement agency

(a) on receipt of a Court order for the disclosure, or

(b) on receipt of the written consent of the subscriber or customer to the disclosure.

Provider to keep logs and records

103. A provider of electronic communication service or remote computing service shall keep logs and records of the

(a) name,

(b) electronic source and destination address,

(c) billing records if any,

(d) duration of service to a subscriber or a customer,

(e) types of services and related logs of the subscribers, and

(f) activities which take place on its electronic platform as may be reasonably appropriate for a period of twelve months.

Backup preservation

104. (1) A Court may order that an electronic communication provider shall create a backup copy of the contents of the electronic communications sought to be preserved on application by a law enforcement agency and the electronic communication provider shall, without notifying the subscriber or customer of the order, create the backup copy and shall confirm to the law enforcement agency that the backup copy has been made.

(2) The law enforcement agency shall within three days after receipt of the confirmation of the creation of the backup, notify the subscriber or customer of the Court order and compliance by the provider.

(3) The provider shall not destroy the backup copy until the delivery of a copy of the backup information to the agency or the determination of the trial in respect of which the back-up application was sought.

(4) Unless notice to vacate the Court order is obtained by the subscriber or customer and served upon the law enforcement agency and the provider, the provider shall release the backup copy to the requesting law enforcement agency fourteen days after receipt of the order for the creation of the backup copy.

Customer challenge

105. A subscriber or customer may apply to a Court to vacate an order obtained under this Act by a law enforcement agency at any time after notice if the Court orders.

Inadmissible evidence

106. Where a Court varies, quashes or modifies an order for disclosure obtained by a law enforcement agency, evidence obtained solely on the basis of that order and not from another independent source is inadmissible in civil, criminal or administrative proceedings.

Cyber offences

Stealing

107. Section 124 of the Criminal Offences Act 1960 (Act 29) on stealing applies with the necessary modification

(a) to any thing done using an electronic processing or procuring procedure system whether or not the appropriation was by use of an electronic processing procedure, and

(b) to any thing whether or not the medium used in the receiving in whole or in part was an electronic record.

Appropriation

108. (1) Section 122(2) of the Criminal Offences Act, 1960 (Act 29) on acts which amount to appropriation applies with the necessary modification to anything whether or not the moving, taking, obtaining, carrying away or dealing is by means of electronic processing or procuring procedure in part or in whole.

(2) For a cyber offence, "thing" includes any electronic related matter which results in the loss of property, identity, electronic payment medium, information, electronic record and any related matter whether tangible or intangible wherever located on any network if the accused is subject to prosecution under this Act.

Representation

109. Section 133 of the Criminal Offences Act, 1960 (Act 29) on false pretences applies with the necessary modification to a representation whether or not the medium used in communicating the representation in part or in whole was an electronic processing system and whether or not the representation consists of an electronic record in part or in whole.

Charlatanic advertisement

110. Section 137 of the Criminal Offences Act, 1960 on charlatanic advertisement in newspapers applies with the necessary modification to any publication in an electronic record, website related publication however described or linked.

Attempt to commit crimes

111. Section 18 of the Criminal Offences Act, 1960 (Act 29) on attempts to commit crimes applies with the necessary modification to any person who attempts to commit a crime whether the medium used in whole or in part was an electronic medium or an electronic agent.

Aiding and abetting

112. Sections 20 and 21 of the Criminal Offences Act, 1960 (Act 29) on abetment of crime applies with the necessary modification to any person who abets a crime whether the medium used in whole or in part was an electronic medium or an electronic agent.

Duty to prevent felony

113. Section 22 of the Criminal Offences Act, 1960 (Act 29) on duty to prevent a felony (Act 29) applies with the necessary modification to any person who knowing that a person plans to commit or is committing a felony, fails to use reasonable means to prevent the commission of the felony whether the medium used in whole or in part was an electronic

medium or an electronic agent and whether the means to prevent the commission of the offence is an electronic medium or agent.

Conspiracy

114. Section 23 of the Criminal Offences Act, 1960 (Act 29) on conspiracy applies with the necessary modification to any person who conspires to commit an offence whether the medium used in whole or in part was an electronic medium or an electronic agent.

Forgery

115. Sections 158, 159,161,162,164,166,167,168,169 and 170 of the Criminal Offences Act, 1960 (Act 29) on forgery apply with the necessary modification to any person who forges anything whether or not the forgery is in whole or in part effected by use of any electronic process or in electronic form.

Intent

116. A person who uses any electronic medium or any electronic agent whether in part or in whole is deemed to intend to cause or contribute to causing the event which results from the use or intervention of the electronic medium or agent.

Criminal negligence

117. A person who uses an electronic medium or any electronic agent whether in part or in whole is deemed to have caused an event negligently if without intending to cause the event, the person causes it by voluntary action from the use or intervention of an electronic medium or agent without the skill and care as are reasonably necessary under the circumstances.

Access to protected computer

118. A person who secures unauthorised access or attempts to secure access to a protected system in contravention of a provision of this Act commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

Obtaining electronic payment medium falsely

119. A person who makes or causes to be made either directly or indirectly, a false representation to procure the issue of an electronic payment medium personally or to another person commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty

units or to a term of imprisonment of not more than ten years or to both.

Electronic trafficking

120. A person who is found in possession of any electronic related payment medium invoices, vouchers, sales drafts, or other representations of devices related to the manufacture or use of the device without lawful explanation commits the offence of electronic trafficking and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

Possession of electronic counterfeit-making equipment

121. A person who receives, possesses, transfers, buys, sells, controls, or has custody of equipment used in the manufacture of counterfeit electronic related materials or electronic record commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

General offence for fraudulent electronic fund transfer

122. A person who without authority, in the course of an electronic fund transfer, uses the personal or financial record or credit account numbers or electronic payment medium of another with intent to defraud an issuer or a creditor or who obtains money, goods, services, or anything fraudulently commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

General provision for cyber offences

123. Except as provided for in this Act, any offence under a law which is committed in whole or in part by use of an electronic medium or in electronic form is deemed to have been committed under that Act and the provisions of that Act shall apply with the necessary modification to the person who commits the offence.

Unauthorised access or interception

124. A person who intentionally accesses or intercepts an electronic record without authority or permission commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both.

Unauthorised interference with electronic record

125. A person who intentionally and without authority interferes with an electronic record in a way which causes the electronic record to be modified, destroyed or otherwise rendered ineffective, commits an offence

and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both.

Unauthorised access to devices

126. A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer programme or a component, which is designed primarily to overcome security measures for the protection of an electronic record, or performs any of those functions with regard to a password, access code or any other similar kind of electronic record, commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both.

Unauthorised circumvention

127. A person who without lawful authority utilises a device or computer programme in order to overcome security measures designed to protect the electronic record or access to it commits an offence and is liable on summary conviction to a fine of more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both.

Denial of service

128. A person who commits any act described in this Act with intent to interfere with access to an information system to effect a denial, including a partial denial of service to legitimate users commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or a term of imprisonment of not more than two years or to both.

Unlawful access to stored communications

129. (1) Whoever, without lawful authority, intentionally accesses a facility through which an electronic communication service is provided, commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

(2) Whoever without lawful authority exceeds an authorisation to access a facility or obtains, alters, or prevents authorised access to a wire or electronic communication while it is in electronic storage in a system

commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

Unauthorised access to computer programme or electronic record

130. (1) A person who knowing and without authority causes a computer to perform any function to secure access to a programme or electronic record held in that computer or in any other computer, commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both.

(2) For the purposes of sections 107 to 141, it is immaterial that the act in question is not directed at

(a) a particular programme or electronic record,

(b) a programme or electronic record of any kind, or

(c) a programme or electronic record held in any particular computer.

(3) A person secures or gains access to a programme or electronic record held in a computer if by causing the computer to perform any function, the person

(a) alters or erases the programme or electronic record,

(b) copies or moves it to a storage medium other than that in which it is held or to a different location in the storage medium in which it is held,

(c) uses it, or

(d) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner,

and references to access to a programme or electronic record and to an intent to secure the access, shall be read accordingly.

(4) A person uses a programme if the function the person causes the computer to perform

(a) causes the programme to be executed, or

(b) is itself a function of the programme.

(5) For the purposes of this Act, the form of any programme or electronic record is immaterial.

Unauthorised modification of computer programme or electronic record

131. (1) A person who does any direct or an indirect act without authority which the person knows or ought to have known will cause an unauthorised modification of any programme or electronic record held in

a computer commits an offence and is liable on summary conviction to a fine of not more that five thousand penalty units or a term of imprisonment of not more than ten years or to both.

(2) It is immaterial that the act in question is not directed at

(a) any particular programme or electronic record,

(b) a programme or electronic record of any kind,

(c) a programme or electronic record held in any particular computer, or

(d) any unauthorised modification is, or is intended to be, permanent or merely temporary.

(3) A modification of a programme or electronic record occurs if, by the operation of a function of the computer concerned or any other computer,

(a) a programme or electronic record held in the computer is altered or erased,

(b) a programme or electronic record is added to or removed from a programme or electronic record held in the computer, or

(c) an act occurs which impairs the normal operation of any computer.

(4) An act which contributes towards causing a modification is regarded as causing it.

(5) A modification is unauthorised if the person who causes it

(a) is not entitled to determine whether the modification should be made,

(b) is not authorised to make the modification or knowingly acted in excess of the authorised modification, or

(c) does not have consent to the modification from the person who is entitled.

Unauthorised disclosure of access code

132. A person who knowingly and without authority discloses a password, access code or any other means of gaining access to a programme or electronic record held in a computer commits an offence and is liable on summary conviction to a fine of not more than ten thousand penalty units or a term of imprisonment of not more than twenty years or to both.

Offence relating to national interest and security

133. (1) Whoever knowingly accesses a computer without authorisation or exceeds authorised access, and by means of the conduct accesses information from a protected computer commits an offence and is liable on

summary conviction to a fine of not more than ten thousand penalty units or to a term of imprisonment of not more than twenty years or to both.

(2) Whoever intentionally accesses a computer without authorisation or exceeds authorised access to a computer which contains

(a) information stored in, transiting through or in the financial records of a financial institution, or consumer reporting agency,

(b) information from a department or agency of the Government,

(c) information from a protected computer, or

(d) information relating to the security of the Republic of Ghana

commits an offence and is liable on summary conviction to a fine of not more than ten thousand penalty units or to imprisonment for a term of not more than twenty years or to both.

(3) Whoever without authorisation or in excess of authorisation by any act, omission, computer hardware or software manipulation or use knowingly causes the transmission of a program, information, code, or command and as a result of the conduct, causes damage to a protected computer commits an offence and is liable on summary conviction to a fine of not more than ten thousand penalty units or to a term of imprisonment of not more than twenty years or to both.

Causing a computer to cease to function

134. A person who intentionally engages in conduct, including virus writing, virus and worm dissemination which causes a computer to cease to function permanently or temporarily commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to imprisonment for a term of not more than ten years or to both.

Illegal devices

135. A person who intentionally, recklessly, without lawful excuse or justification, possesses, produces, sells, procures for use, imports, exports, distributes or otherwise makes available

(a) a device, including a computer programme, that is designed or adapted for the purpose of committing an offence, or

(b) a computer password, access code or similar electronic record by which the whole or any part of a computer system is capable of being accessed

with the intent that it be used by a person for an offence commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

Child pornography

136. (1) A person who intentionally does any of the following acts:

(a) publishes child pornography through a computer;

(b) produces or procures child pornography for the purpose of its publication through a computer system; or

(c) possesses child pornography in a computer system or on a computer or electronic record storage medium

commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both.

(2) In this section:

"child pornography" includes material that visually depicts

(a) a child engaged in sexually explicit conduct;

(b) a person who appears to be a child engaged in sexually explicit conduct;

(c) images representing a child engaged in sexually explicit conduct; and

(d) unauthorised images of nude children;

"child" means a person below eighteen years;

"publish" means

(a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph *(a)*; and

(c) print, photograph, copy or make in any other manner whether of the same or of a different kind or nature to carry out an act referred to in paragraph *(a).*

Confiscation of assets

137. A Court may order the confiscation of moneys, proceeds, properties and assets purchased by a person with proceeds derived from or in the commission of the offence on the conviction of the person for an offence under this Act and may further order the return of any money or thing to any victim of the crime.

Order for compensation

138. (1) A Court may make an order against a person for the payment of a sum to be fixed by the Court as compensation to be paid by the person to any person for damage caused to that person's computer, program or electronic record as a result of the offence for which the sentence is passed.

(2) A claim by a person for damages sustained because of the offence shall be deemed to have been satisfied to the extent of an amount which has been paid to the person under an order for compensation, but the order shall not limit any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(3) An order for compensation under this section is recoverable as a civil debt.

Ownership of programme or electronic record

139. A programme or electronic record held in a computer is deemed to be property of the owner of the computer.

Conviction and civil claims

140. A conviction shall not limit the right of a complainant to bring a civil action.

Record and access to seized electronic record

141. (1) If a computer or electronic record has been removed or rendered inaccessible after a search or a seizure under this Act, the person who made the search shall, at the time of the search or as soon as practicable after the search,

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure, and

(b) give a copy of that list to

(i) the occupier of the premises, or

(ii) the person in control of the computer.

(2) The police officer or another authorised person may refuse to give access or provide copies if giving the access, or providing the copies

(a) would constitute a criminal offence, or

(b) would prejudice

(i) the investigation in connection with which the search was carried out,

(ii) another ongoing investigation, or

(iii) criminal proceedings that are pending or that may be brought in relation to any of those investigations.

Territorial scope of offences under this Act

142. (1) This Act has effect in relation to a person of whatever nationality outside as well as within the country and where an offence under this Act is committed by a person in any place outside the country, the person may be dealt with as if the offence had been committed within the country.

(2) This Act shall apply if, for the offence in question

(a) the accused was in the country at the material time;

(b) the electronic payment medium, computer or electronic record was issued in or located or stored in the country at the material time;

(c) the electronic payment medium was issued by a financial institution in the country; or

(d) the offence occurred within the country, on board a Ghanaian registered ship or aircraft or on a voyage or flight to or from this country at the time that the offence was committed, whether paragraph *(a), (b)* or *(c)* applies.

Regulations

143. The Minister may by legislative instrument make regulations

(a) to define, enlarge or restrict the meaning of a word or expression used in this Act;

(b) to specify provisions of or requirements under another enactment to which this Act does not apply;

(c) to prescribe records, information or classes of records or information not applicable to this Act;

(d) to prescribe records or classes of records for which a requirement under law for the signature of a person must be satisfied by an electronic signature and proof that, in view of the circumstances including any relevant agreement and the time the electronic signature was made,

(i) the electronic signature is reliable for the purpose of identifying the person, and

(ii) the association of the electronic signature with the relevant electronic record is reliable for the purposes for which the electronic record was made;

(e) to provide for electronic signatures;

(f) to provide for the electronic means to be used to send, receive or retain information or records in electronic form if

an enactment requires a person to send, receive or retain the information or records; and

(g) to provide for any other matter necessary for the effective implementation of this Act.

Interpretation

144. In this Act, unless the context otherwise requires,

"access" includes the actions of a person who, after taking note of data, becomes aware of the fact that there is no authorisation to access that data and still continues to access that data;

"addressee", in respect of an electronic record, means a person who is intended by the originator to receive the electronic record, but not a person acting as an intermediary with respect to that electronic record;

"authentication products or services" means products or services designed to identify the holder of an electronic signature to other persons;

"authentication service provider" means a person whose authentication products or services have been accredited by the Certifying Agency under this Act;

"Agency" means the National Information Technology Agency;

"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of electronic records in which the conduct or electronic records of one or both parties are not reviewed by an individual in the ordinary course of the individual's business or employment;

"Board" means Board of the Agency;

"browser" means a computer programme which allows a person to read hyperlinked electronic records;

"cache" means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or processing;

"ccTLD" means country code domain at the top level of the Internet's domain name system assigned according to the two-letter codes in the International Standard ISO 3166-1 (Codes for Representation of Names of Countries and their Subdivision);

"certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with an electronic record;

"Certifying Agency" means the Certifying Agency established under this Act;

"clear days" means complete days excluding the day of dispatch.

"computer" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, performs automatic processing of data or any other function but does not include

(a) portable hand held calculator,

(b) an automated typewriter or typesetter,

(c) a similar device which is non-programmable or which does not contain any data storage facility, or

(d) any other device that the Minister may prescribe in the *Gazette*;

"computer output" or "output" means a statement or representation, whether in written, printed, pictorial, graphical, electronic, digital or any other form, purporting to be a statement or representation of fact

(a) produced by a computer, or

(b) accurately translated from a statement or representation so produced,

"computer service" includes computer time, computer output, data processing and the storage or retrieval of a programme or data;

"consumer" means an individual person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"controller" means a person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

"Court" means any judicial, quasi-judicial or other administrative tribunal established by law;

"critical database" means a crucial set of data in an electronic record related to national security or the economic well being of the public determined by the Minister;

"critical database administrator" means the person responsible for the management and control of a critical database;

"critical electronic record" means an electronic record, group or classification of electronic record which is declared by the Minister to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens;

"cyber inspector" means a staff of the National Information Technology Agency with power to monitor, investigate, prosecute any offence under this Act and any other law enforcement agency acting under any provision of this Act;

"damage", includes impairment to a computer or the integrity or availability of a programme or data held in a computer that

(a) causes loss within the period prescribed under the Limitation Decree, 1972 (N.R.C.D. 54),

(b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of a person,

(c) causes or threatens physical injury or death to a person, or

(d) threatens the public interest;

"decryption information" means information or technology that enables a person to readily retransform or unscramble an encrypted programme or data from its unreadable and incomprehensible format to its plain text version;

"device" means any thing or apparatus that is used or capable of being used to intercept a function of a computer or electronic record;

"digital signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;

"domain name" means an alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the Internet;

"domain name system" means a system to translate domain names into IP addresses or other information;

"e-government services" means a public service provided by electronic means by a public body in the country;

"e-mail" means electronic mail, an electronic record used or intended to be used as a mail message between the originator and addressee in an electronic communication;

"electronic agent" means a computer programme or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, in an automated transaction;

"electronic communication" means a communication by means of electronic records;

"electronic payment medium" includes any medium issued to a holder capable of being used to make an electronic financial transaction;

"electronic record" includes data generated, sent, received or stored by electronic means

(a) voice, where voice is used in an automated transaction; and

(b) a stored record;

"electronic transaction" means a transaction by an electronic agent;

"encrypted product" means a product that makes use of encryption techniques and is used by a sender or recipient of electronic record to ensure

(a) that the data can be accessed only by relevant persons,

(b) the authenticity of the data,

(c) the integrity of the data, or

(d) that the source of the data can be correctly ascertained;

"encrypted programme or electronic record" means a programme or data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilized for the transformation or scrambling and irrespective of the medium in which the programme or data occurs or can be found for the purposes of protecting the content of the programme or data;

"encryption provider" means any person who provides or who proposes to provide encryption services or products in the country;

"encryption service" means a service which is provided to a sender or a recipient of an electronic record or to anyone storing an electronic record, which is designed to facilitate the use of encryption techniques to ensure

(a) that the data or electronic record can be accessed or can be put into an intelligible form only by certain persons,

(b) that the authenticity or integrity of the data or electronic record is capable of being ascertained,

(c) the integrity of the data or electronic record, or

(d) that the source of the data or electronic record can be correctly ascertained,

"essential emergency service" means a vital service to avoid the imminent occurrence of a situation which is out of the ordinary which threatens to endanger a person, public safety or cause damage to property;

"financial institution" means an entity that undertakes financial intermediation;

"financial intermediation" means a process of transferring funds from one entity to another entity;

"Forum" means Industry Forum;

"function" includes logic, control, arithmetic, deletion, storage and retrieval, and communication or telecommunication to, from or within a computer;

"*Gazette*" includes an electronic record of the *Gazette* and publication on the website of the appropriate Government Agency;

".gh domain name space" means the .gh ccTLD assigned to the Republic according to the two-letter codes in the International Standard ISO 3166;

"Government" means any authority by which the executive authority of the Republic is duly exercised;

"home page" means the primary entry point webpage of a web site;

"hyperlink" means a reference or link from some point in one electronic record directing a browser or other technology or

functionality to another electronic record or point in that electronic record or to another place in the same electronic record;

"hyper text" means a reference or link from some point in one electronic record directing a browser or other technology or functionality, to another electronic record or point or to another place in the same electronic record;

"incorporated body" means an entity registered under the Companies Code 1963 (Act 179), the incorporated Private Partnerships Act 1962 (Act 152) or the Trustees Incorporation Act, 1962 (Act 106);

"industry " means the communications industry;

"Industry Forum" means the communications industry meeting from time to time to discuss matters of common interest to and concerning the industry;

"information system" includes a system for generating, sending, receiving, storing, displaying or otherwise processing electronic records and the Internet;

"information system services" includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of electronic records between or among points specified by a user and the processing and storage of data at the individual request of the recipient of the service;

"intercept" includes, in relation to a function of a computer or electronic record, listening to or recording a function of a computer or electronic record, or acquiring the substance, meaning or purport of it;

"intermediary" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular electronic record or provides other services with respect to that electronic record;

"Internet" means the interconnected system of networks that connects computers around the world using the TCP/IP and future versions of the inter connected system;

"IP address" means the number identifying the point of connection of a computer or other device to the internet;

"law enforcement agency" means the police, customs, excise and preventive service and any other law enforcement agency authorised by law to exercise police powers;

"Minister" means the Minister responsible for Commu-nications;

"Ministry" means the Ministry responsible for Commu-nications;

"originator" means a person by whom, or on whose behalf, an electronic record purports to have been sent or generated prior to storage, but does not mean a person acting as an intermediary with respect to that electronic record;

"person" includes a public agency;

"personal information" means information about an identifiable individual, including, but not limited to

(a) information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being; disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol, or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made

to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than twenty years;

"plain text version" means a programme or original data before it has been transformed or scrambled to an unreadable or incomprehensible format;

"prescribe" means prescribe by regulation under this Act;

"programme or computer programme" means data representing instructions or statements which when executed in a computer, causes the computer to perform a function;

"programme or data" includes a reference to a programme or data held in any removable storage medium which is for the time being in the computer;

"public agency" means a body set-up by Government in the public interest with or without an Act of Parliament;

(a) department of central government or a department in local government; or

(*b)* any other functionary or institution when

(i) exercising a power or discharging a duty in terms of the Constitution; or

(ii) exercising a power or performing a function in terms of any legislation;

"public key" means the key which is available to the public for purposes of the encryption of an electronic key which is linked to a private decryption key held exclusively by the issuer of the key available to the public;

"public interest" includes a right or advantage which enures or is intended to enure to the general benefit of the people of this country;

"registrar" means an entity which is licensed by the Registry under this Act;

"Registry" means an entity licensed by the Registrar to manage and administer a specific sub domain;

"repository" means the primary register of the information maintained by a registry;

"second level domain" means the sub domain immediately following the ccTLD;

"security agency" means a body connected with national security;

"service provider" means any person providing information system services.

"statutory provision" means by or under an Act of Parliament;

"sub domain" means any subdivision of the .gh domain name space which is the second level domain;

"TCP/IP" means the Transmission Control Protocol Internet Protocol used by an information system to connect to the Internet;

"TI-D" means a top level domain of the domain name system;

"third party", in relation to a service provider, means a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems;

"transaction" means a transaction of either a commercial or non-commercial nature and the provision of information and e-government services;

"unauthorised access" is access of any kind by a person to a programme or data held in a computer without authority if

(a) the person is not personally entitled to control access of the kind in question to the programme or data; and

(b) the person does not have consent to access the kind of programme or data from the person who is entitled to control access;

"unincorporated body" means an entity registered under the Registration of Business Names Act, 1962 (Act 151) or any person carrying on business without a registration or without a certificate of incorporation;

"universal access" means access by all citizens of Ghana to internet connectivity and electronic transactions;

"webpage" means an electronic record on the World Wide Web;

"website" means a location on the Internet containing a home page or web page; and

"World Wide Web" means an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer.

MEMORANDUM

This Bill forms part of the e-legislation package for statutory authority for the 2005 National Telecom Policy to provide a legal framework for electronic transactions amongst others. The Bill provides for and facilitates electronic communications and related transactions in the public interest and applies to all electronic transactions and electronic records.

It is the object of Government to facilitate the use of electronic media to speed up government and private business in recognition of the need to provide a framework for the preparation, processing, storage, transmission and receipt of electronic data in a secured, efficient, trustworthy manner. Furthermore, Government desires to prevent the use of electronic media for illegal or unlawful acts.

The Bill is divided into twelve groups of clauses. These deal with electronic transactions, electronic government services, the certifying agency and consumer protection. Other groups of clauses relate to the Appeal forum, Industry forum, the duties of service providers and cyber offences.

The first group of clauses, clause 1 – 4 sets the framework for the Bill by providing the object of the legislation, application and scope of the Bill.

The second group of clauses, clause 5 - 24 deals with electronic transactions and provides for the recognition and admissibility of electronic records and electronic signatures, the recognition of electronic certificates, electronic notarisation, acknowledgement and certification services, and automated transactions, clause 5 – 17.

Electronic documents will satisfy the requirement of writing imposed by any law and will not be denied admissibility in evidence if they are accessible and capable of being retained for subsequent reference. Where the law requires multiple copies of a document to be submitted to a single

addressee at the same time, that requirement will be satisfied by the submission of a single electronic record that is capable of being reproduced by that addressee, clause 16. A requirement by law that a document be signed by a person will be satisfied in relation to an electronic document if an electronic signature is used. The Bill specifies what constitutes an authentic electronic signature in clause 16.

Agreements concluded partly or wholly through an electronic medium are not of themselves invalid. For the purpose of electronic transactions, an electronic agent may be involved at any stage except that a party dealing with an electronic agent is not bound by the terms of the agreement unless terms were first capable of being accessed by the party prior to the formation of the contract, clause 17.

The Bill also deals with the time and place of despatch and receipt of electronic records. Under clause 18 the despatch of an electronic record occurs when it enters an information processing system outside the control of the originator, unless otherwise agreed between the originator and the addressee. Under clause 19, receipt occurs at the time when the electronic record enters the designated information system of the addressee, unless otherwise agreed. If the addressee has not designated an information system, receipt occurs when the electronic record enters an information system of the addressee or through which the addressee retrieves its electronic record.

The place of despatch of an electronic record is deemed to be the originator's registered place of business, and deemed to be received at the addressee's registered place of business, unless otherwise agreed, clause

Date of *Gazette* notification: 19th December, 2008.

GOVERNMENT PRINTER, ASSEMBLY PRESS, ACCRA. GPC/A727/300/12/2008

This printed impression has been carefully compared by me with the Bill which has been passed by Parliament, and found by me to be a true copy of that Bill.

Clerk to Parliament

Date of authentication:

I hereby signify assent to this Bill.

President

Date of Assent:

19. The Bill also clarifies in clause 21 how electronic documents may be attributed to an originator.

The third group of clauses, clause 25 - 27 provides for e-Government service which is public service provided by electronic means by a public body. A public body is empowered by any law in clause 26 to accept for filing, accept payment, issue permits, licences or approvals by electronic means. The Bill does not seek to compel public bodies to process electronic records, clause 25. A public body may however publish in the *Gazette* details of the manner and format in which it will accept and retain electronic records. The Bill also allows for the publication of the Official *Gazette* in electronic format, clause 27.

The fourth group of clauses, clause 28 – 45 is on the Certifying Agency which is to certify encryption or authentication services provided in the country and monitor the conduct, systems and operations of encryption and authentication service providers. The functions of the Certifying Agency are provided in clause 31. Service and products of persons certified by a Certifying Foreign Agency recognised by the local Agency will be allowed, clause 34. Among other things, the Agency is also to act as the repository of Digital Signature Certificates issued under this Bill and maintain a computerised database of public keys to make them verifiable by a member of the public, clause 35.

Consumer protection is dealt with in the fifth group of clauses, clause 46 – 54, which provides for the protection of consumers in electronic transactions. The obligations of suppliers offering goods or services for sale, hire or exchange to consumers on an electronic platform are spelt out in clause 47. For instance, consumers will be entitled to information relating to the supplier and the goods or services offered. Suppliers will be duty-bound to utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction according to the type of transaction concerned. Suppliers will be liable for any damage suffered by a consumer due to a failure by the supplier to apply a sufficiently secure payment system. Unsolicited goods, services, and communications are prohibited in clause 50. Financial institutions are not to make available, lend, or sell a list or portion of a list of holders of any electronic payment medium and their addresses and account numbers to any person without the prior written consent of the holders, clause 51. This will be subject to other laws related to credit reporting.

88 – 89. It will be a platform that brings the industry together from time to time to discuss matters of common interest to and concerning the industry. The National IT Agency may designate an industry body to be the forum, clause 87. The forum may prepare a voluntary industry code on its own initiative or upon request by the Agency clause 89.

The liability for service providers is imposed in the tenth group of clauses, clause 90 – 96. It imposes liabilities on service providers for electronically published matter that is illegal or unlawful. Other acts are prohibited such as knowingly divulging to any person or entity the contents of a communication while in electronic storage by that service, clause 96. It excludes from liability, intermediaries who merely provide access to, transmit, or store/host electronic records under specified conditions. A person claiming that any electronically published matter is illegal or unlawful may notify the publisher and request that it be taken down, (clause 94). An intermediary or service provider is generally speaking, not required to monitor an electronic record processed by means of the system in order to ascertain whether its processing will constitute or give rise to an offence or give rise to civil liability, clause 92.

Law enforcement is dealt with in the eleventh group of clauses which adds to the powers of arrest, search, and seizure of law enforcement agencies by law. The Bill empowers law enforcement agents in the course of the execution of court warrants to seize a computer, electronic record, programme, information, document or thing if they reasonably believe that it is evidence that an offence under the Bill has been or is about to be committed, clause 98. Law enforcement agencies may also request the preservation of evidence by providers of wire or electronic communication services or a remote computing service pending the issuance of a Court Order or other process clause 100. Controls against incrimination are provided for under the Bill. The Court is empowered, upon application of a law enforcement agency, to order an electronic communication service provider to disclose the contents of an electronic communication, that is in transit, held, maintained or has been in electronic storage in an electronic communications system, if the disclosure is relevant and material for investigative purposes or is in the interest of national security, clause 101.

Cyber offences are contained in the twelfth group of clauses, clause

Illegal access to protected computers is dealt with in the sixth group of clauses clause 55 – 62. Information contained in the register of a critical database is not to be disclosed to any person other than to the relevant employees of the National Information Technology Agency, clause 60.

Protected computers and critical database which have been declared by government are not to be accessed illegally. The protection extends to computers and databases for national security, defence, public safety and public health, emergency systems. Databases relating to the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure, or used by the legislative, executive and judicial arms of government, the public services and security agencies are also designated as critical under the Bill, clause 55.

Provisions on the domain name register are in the seventh group of clauses. A domain name Registry is established to assume responsibility for the ".gh" country domain name space from a date to be determined by the Minister by notice in the *Gazette.* After the commencement of the Act, a person shall not update a repository or administer a second level country domain name unless the person is licensed to do so by the Registry. The governing body of the Registry is a Board composed of nine members and may be converted into a company limited by guarantee, clause 63. Its functions will include the administration and management of the ".gh" domain name space. It will license and regulate registrars for the respective registries and publish guidelines on the general administration and management of the ".gh" domain name space.

The eighth group of clauses, clause 82 – 87 provides for an appeal tribunal and establishes the Information Communication Technology Tribunal in clause 81. This will be convened on an adhoc basis to consider appeals against decisions of the National Information Technology Agency. The three member tribunal is to be appointed by the Chairperson of the Public Services Commission, clause 72. The expenses of the tribunal will be paid out of income derived by the Agency and will be part of the annual budget of the Agency. Decisions of the tribunal relating to points of law can be appealed against to the Court of Appeal clause 87.

An industry forum is estab he ninth group of clauses clause

107 – 140. The provisions of the Criminal Code are extended to cover various offences committed through electronic means. These offences include stealing, appropriation, charlatanic advertisement and dishonest receiving. Others are attempt to commit crimes, aiding and abetting, conspiracy, forgery and criminal negligence. The publication of child pornography by electronic means is also criminalised.

In addition to these, access to protected computers, obtaining electronic payment medium falsely, electronic trafficking, possession of electronic counterfeit-making equipment are offences. Fraudulent electronic fund transfer, unauthorised access or interception, unauthorised interference with electronic records, unauthorised access to devices are also offences. The rest include unlawful access to stored communications, unauthorised circumvention, causing a computer to cease to function and child pornography. Conviction for these offences attracts heavy fines and long terms of imprisonment

The last group of clause is on miscellaneous matters and contains a general provision to the effect than an act which constitutes an offence under a law here which is committed wholly or partly by use of an electronic medium or in electronic form outside the country will be dealt with as if the offence had been committed here. This group also contains the powers to make Regulations and the interpretation clause.

DR. BENJAMIN AGGREY NTIM
Minister for Communications

Date: 8th May, 2008.

Electronic Transactions Bill