Chapter 2

Legal and Socio-Ethical Issues in Online Business

2.1 Introduction

This chapter reviews and discusses legal and socio-ethical requirements that affect Online Business activities. There is particular reference to Internet law with respect to interpretations of different aspects of the Law. Some of the laws covered in the chapter includes, Fraud and Abuse Act of 1986, Computer Misuse Act of 1990, Copyright, Electronic Communication Privacy Act 2000 and the data protection Act of UK 2000. Email and Privacy Laws usually covering email policy, email privacy, monitoring employees, Right of Privacy in Online applications, Crypto-systems, Online Games and Gambling, and most importantly the Telephone consumer Act of 1991.

2.2 Legislation and Law

The global reach of the Internet makes it an ideal tool for international business beyond traditional business channels in an information society. The rapid deployment of commercial web sites globally shows the importance of this cost-effective possibility for businesses to present themselves in a global market place, Bernard Glasson et al (30, 31, 34). In view of this new marketing and business age, using sophisticated technology in Online business activities have become more complex than the years before. The law regulating the behaviour of individuals and businesses with the advent of advance technology in this regard is not as effective as one will expect it to be, within the broader context of international law.

In his article "net can't catch cyber criminals" Rob Jones expressed the worries and frustrations of Albert Pacey the director general of the national criminal intelligence service (NCIS) UK. The boss of the intelligence service warned that it was needed to criminalise the theft of electronic data. He was speaking to delegates from police forces around the world, at the organised crime conference in London to discuss how they combat the (IT) criminal class. To summarise his words, he said "change the law or face the growth of a new criminal class" Jones R (1997).

In retrospect the NCIS boss's proposition was arguably valid in the sense that looking into the embedded issues of security for funds transfer and information in general, the possible solutions lies in the hands of Governments rather than information technologists. It is Governments because, the issue is international not national. Any approach used by a particular nation's Government to resolve this issue which reflects a national approach is more likely to fail. In view of this, there is the need to adopt a strategy that takes into consideration specific countries legal framework and culture. This is because we are in a global economic information age, as such all issues surrounding security of Online Business should be addressed globally. It will therefore be just an illusion of success if a global approach is not adopted.

Although the electronic communications privacy act of 1986 specifically forbids eaves dropping on electronic transmissions, laws of that kind are extra-ordinarily difficult to enforce, because no policing agency controls the points of access Spar D and Jeffery J (1996). Since the core cause of this problem is international rather than national, it will be very much appropriate for us to examine the impact of international law on this issue.

2.2.1 International Law

The simplest definition of international law believed ever defined is "a system of rules governing the relations between sovereign states". Let us take a particular interest in the word sovereign or sovereignty Dixon M (306, 138, 276). According to the oxford dictionary, it means supremacy, self Government or a self Governing State. It is important for us to note that for the sovereignty of a state to be recognised in the purview of law, its jurisdiction must be clearly defined.

Jurisdiction is the extent of a nation's legal or territorial authority. In other words where it can administer justice, play a crucial role in the contribution to information security management of Online Business. This is because globalisation of information transfer cuts across the boundaries of nations.

2.2.1.1 Limitations of International Law

It is the limitation of international law in this regard why concerned people like Albert Pacey, and other passionate members of the information research community fear that current state of cyber-crime if not managed

effectively will get out of hand. Although some part of the law empowers nations to arrest and prosecute individuals who might commit a crime against any of its institutions. It only works where the criminal's nation or where s/he takes refuge corporate in the arrest and prosecution. It must be noted that this aspect of the law mostly applies exclusively outside the scope of information technology, due to the fact that laws covering computer crime needs further development and enforcement globally. In order for us to get a better picture concerning this aspect of the law, let us examine the Harvard research convention on jurisdiction with respect to crime (1935). "A state has jurisdiction with respect to any crime committed outside it's territory by an alien against the security, territorial integrity or political independence of that state, provided that the act or omission which constitutes the crime was not committed in exercise of a liberty guaranteed the alien by law of the place where it was committed".

Social order and the coexistence of states make it important for boundaries between their sovereignties and jurisdictions. This is because contradiction of every state's power is inevitably involved. The American law institute defines jurisdiction as "the capacity of a state under international law to prescribe or enforce a rule of law". The institute's definition draws attention to the distinction between a state's jurisdiction to prescribe and to enforce law. A state can not enforce a law it has no right to prescribe. However a state may prescribe a law it may be unable to enforce. For instance if a criminal commits a crime and escapes into another states jurisdiction, and that state has no good international relations with state that the crime was committed against, the affected state has no right to extend it's judicial powers in that state Levi W (107).

Poor international relations grossly contribute to the ineffectiveness of the law. It is a real unforeseen menace that lies ahead of Online Business global community.

There are independent organisations that provide advice to consumers with respect to these Acts. These organisations include; The Online Privacy Alliance, (AUCE) European coalition for unsolicited emails, Crypto Law Society and Australian Privacy Foundation. Section 1.6 presents the Electronic Communication Privacy Act as applied in the USA. This is designed to provide relevant information regarding the legal implications in case of violation or an incident of abuse with respect to privacy in places where similar Acts of Law exist. You may skip this section if you are already familiar with this particular Act.

2.2.2 Internet Law

Section 2.1.1 presents a compilation from Phillips Nizer LLP (2007) on Electronic Communication Privacy Act 47 U.S.C Section 230, Electronic Communications Privacy Act, Stored Wire and Electronic Communications and Transactional Records Access.

18 U.S.C. §§ 2701-2711

§ 2701. Unlawful Access to Stored Communications

(a) Offence - Except as provided in subsection (c) of this section whoever -

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment - The punishment for an offence under subsection (a) of this subsection is -

(1) if the offence is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain -

(A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offence under this subparagraph; and

(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offence under this subparagraph; and

(2) a fine under this title or imprisonment for not more than six months, or both, in any other case.

(c) Exceptions - Subsection (a) of this section does not apply with respect to conduct authorized

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

§ 2702. Disclosure of Contents

(a) Prohibitions - Except as provided in subsection (b) -

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

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

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(b) Exceptions - A person or entity may divulge the contents of a communication

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

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

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

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

(6) to a law enforcement agency -

(A) if such contents -

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime.

(B) if required by section 227 of the Crime Control Act of 1990.

§ 2703. Requirements for Governmental Access

(a) Contents of Electronic Communications in Electronic Storage - A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Electronic Communications in a Remote Computing Service -

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection -

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity -

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service -

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purpose of providing any services other than storage or computer processing.

(c) Records Concerning Electronic Communication Service or Remote Computing Service -

(1)(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity -

(i) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

(ii) obtains a court order for such disclosure under subsection (d) of this section;

(iii) has the consent of the subscriber or customer to such disclosure; or

(iv) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title).

(C) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the name, address, local and long distance telephone toll billing records, telephone number or other

subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under subparagraph (B).

(2) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for Court Order - A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A) and shall issue only if the governmental entity offers specific facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter - No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

(f) Requirement to Preserve Evidence -

(1) In general - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewed request by the governmental entity. §2704. Backup Preservation.

(a) Backup Preservation -

(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of (A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider -

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity. (5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer Challenges -

(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber

or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement -

(A) stating that the application is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) Stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications

sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken there from by the customer. §2705. Delayed Notice

(a) Delay of Notification -

(1) A governmental entity acting under section 2703(b) of this title may -

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is -

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that -

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber -

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of Notice to Subject of Governmental Access - A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in -

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§2706. Cost Reimbursement

(a) Payment - Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount - The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception - The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court

determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§ 2707. Civil Action

(a) Cause of Action - Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) Relief - In a civil action under this section, appropriate relief includes -

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages - The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) Disciplinary Actions for Violations - If a court determines that any agency or department of the United States has violated this chapter and the court finds that the circumstances surrounding the violation raise the question whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department concerned shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee.

(e) Defence - A good faith reliance on -

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defence to any civil or criminal action brought under this chapter or any other law.

(f) Limitation - A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

§ 2708. Exclusivity of Remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for no constitutional violations of this chapter.

§2709. Counterintelligence Access to Telephone Toll and Transactional Records

(a) Duty to Provide - A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required Certification - The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director, may -

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that -

(A) the name address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that -

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with -

(i) an individual who is engaging or has engaged international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.

(c) Prohibition of Certain Disclosure - No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by Bureau - The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement That Certain Congressional Bodies Be Informed - On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

§ 2710. Wrongful Disclosure of Video Tape Rental or Sale Records

(a) Definitions - For purposes of this section -

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfilment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video Tape Rental and Sale Records -

(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d);

(2) A video tape service provided may disclose personally identifiable information concerning any consumer -

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if -

(i) the video tape service provider had provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video taper service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if -

(i) the consumer is given reasonable notice, by the person seeking the disclosure of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure. If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil Action -

(d) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court

(e)(2) The court may award -

(A) actual damage but not less than liquidated damages in an amount of $2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(f) Personally Identifiable Information - Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State or a political subdivision of a State.

(g) Destruction of Old Records - A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(h) Preemption - The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

§ 2711. Definition for chapter

As used in this chapter -

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communication system.

Source: http://www.phillipsnizer.com/library/topics/computer_fraud.cfm: accessed: 25/01/2007. A compilation by Martin Samson

2.3 Social and Ethical Issues

Although society abhors fraud and accepts that it is wrong and should be prevented. The methods that are used to detect or prevent fraud sometimes conflict with the law and also violate the right of the individual's privacy. This section examines certain factors that restrain the effective application of methods developed and devised to detect or prevent crime. **Privacy** is one of such factors. A method such as data marching of personal records compiled for unrelated purposes actually violates the data processing act 1984 that have subsequently been reviewed since 1992, 1998 and 2000. Despite that this is supported by the Act, end users have the right to control personal information and prevent its use without consent for purposes unrelated to those for which it was collected. **The due process of the law**, also makes it difficult for the individual not to be notified in a situation where data marching have taken place and has been found to fall in a category where he is possibly viewed as a potential fraudulent person. Since notifying the individual might affect the investigation, his right for justice in most instances is curtailed.

Although it might affect the course of the investigation, apprehending or arresting people on the grounds of data marching on possibly an insecure computer system mounted somewhere is ethically wrong. If we, persons of information systems management background, view this as ethically incorrect, what will be the ordinary person's view. It will certainly be seen as a humiliation and a miscarriage of justice in any form. As a result of this societal response, the security of distant funds transfer and other banking

activities are sometimes crippled by this social issue, as such crimes are committed without anyone being held responsible. “Power imbalance or power in the wrong hands”. This is how we term it, because too much power has been given to ordinary people to explore technology to any extent to which they desire. If there will be improvement in the security management of information then the power balance much change. Internal controls must be highly improved and co-ordinated through all banking institutions. Companies are marketing their products at the expense of information security, in view of this Governments must review policies that control the operations of businesses.

2.4 Summary

Chapter 2 discussed legal issues on Online transactions and electronic security by providing key references to independent organisations that sought the interest of consumers. References were also made to common acts of the legislature adopted globally. A compilation by Martin Samson on interpretations of internet law was presented. The chapter focused on internet law because the author believed that it was essential that stakeholders of Online Business understood the implications of internet law on Online Business since it constituted an important aspect of the legal framework.

http://www.springer.com/978-0-387-35771-3

Online Business Security Systems
Williams, G.B.
2007, XVIII, 220 p., Hardcover
ISBN: 978-0-387-35771-3