UNIVERSITY OF JOHANNESBURG

FACULTY	: Law
DEPARTMENT	: Private Law
CAMPUS	: APK
MODULE	: CYL41Y0 Cyber Law
SEMESTER	: Second
EXAM	: JANUARY

DATE	:	**SESSION**	: 08:30-10:30
ASSESSOR(S)	: Prof M Njotini		
MODERATOR	: Prof S Nel		
DURATION	: 3 HOURS	**MARKS**	: 100

NUMBER OF PAGES: 9 PAGES

INSTRUCTIONS:

1. Answer ALL THE QUESTIONS.
2. Number your answers clearly

Question 1

1.1 The fact that data refers to the electronic representation of information in any form means, for information representation purposes, that information can, generally, be represented either manually or electronically. Manual representation relies on the paper-based method. Whereas, electronic representation implies the online-based representation of information. (5)

1.2 Technological convergence refers to the merging of telephone, broadcasting and computing or digital technologies. It includes a combination of the nature and architecture of these computing technologies.

Legal convergence depends on two propositions. The first deals with the extension of the freedoms accruing online to the Internet. The second has to do with the communicative values and codes to be used as tools to regulate or manage online activities. (5)

1.3

1.3.1 In terms of the National Cybersecurity Policy Framework, cybercrime is the illegal acts, the commission of which involves the use of information and communication technologies. (2)

1.3.2 The National Cybersecurity Policy Framework defines cybersecurity very broadly. It states that cybersecurity is the practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them. (3)

1.4 The idea to promote a cybersecurity culture is dealt with in paragraph 14 of the National Cybersecurity Policy Framework, 2015. In terms of this paragraph, this promotion has to consider a number of factors. These are that:

- It must deal with the implementation of Cybersecurity awareness programs for private sector, public sector and civil society users.
- It must encourage business to develop a positive culture for Cybersecurity.
- It has to support outreach to civil society, children and individual users.

- It ought to promote a comprehensive national awareness program and guideline.
- It must cover the reviewing and updating existing privacy regime(s).
- It should aim to develop awareness of existing or looming cyber risks and the available solutions.
- It must review, on a continuous basis, cyber applications and the impact from a Cybersecurity perspective.
- It must compliment the culture of cybersecurity with online support mechanisms. (10)

1.5

1.5.1 Section 14 of the Constitution of the Republic of South Africa, 1996 aims to maintain the privacy and sanctity of data. In general, this section covers the right to privacy by providing that "the right to privacy includes everyone's right not to have their person or home searched, their property searched, their possession seized, or the privacy of their communications infringed". The Constitutional Court in the case *NM v Smith* 2007 (5) SA 250 (CC) gave content and meaning to this right. This court stated that:

"Although as human beings we live in a community and are in a real sense both constituted by and constitutive of that community, we are nevertheless entitled to a personal sphere from which we may and do exclude that community. In that personal sphere, we establish and foster intimate human relationships and live our daily lives. This sphere in which to pursue our own ends and interests in our own ways, although often mundane, is intensely important to what makes human life meaningful". (5)

1.5.2 The object and purpose of the Principles or Conditions for the Lawful Processing of Information is to regulate the manner of preserving the integrity of data. Furthermore, they deal with the management of the process relating to how data is collected and processed. In this manner, the principles respond to the necessity to preserve the sanctity of data. Section 4 of the Protection of Personal Information Act 4 of 2013 is pivotal in this regulatory exercise. This section specifically sets out these principles or conditions. These are accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. (5)

1.5.3 Information quality relates to the taking of measures to assure that the data is complete, accurate, not misleading, and updated (up-to-date). It is essential that the measures must be reasonably practicable. An objective test is thus applied to determine whether the measures are reasonable practicable. This has to do with examining all the relevant factors to establish exactly what was actually done to ensure that data is complete, accurate, not misleading and updated.

Openness is a direct opposite of secrecy. This principle promotes the processing of data in a transparent manner. Thus, responsible parties should keep all the documentations associated with the processing of data. In turn, data subjects must be aware of the processing operations and procedures of a responsible party. In addition, the principle requires the responsible party to consider the reasonable practical steps encapsulated in section 18(1) of POPI Act. These include the following:

- Informing the data subject about information being collected and where the information is not collected from the data subject, the source from which the information is collected.

- Informing the data subject about the name and address of the responsible party, purpose for which the information is being collected, whether or not the supply of the information by the data subject is voluntarily or mandatory

- Informing the data subject about the consequence of the failure to provide the data, and any particular law authorising or requiring the collection of the data.

- The data subject to be made aware of the fact that, where applicable, the responsible party intends to transfer the data to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation, and any supplementary information necessary to ensure that the processing of data is reasonable.

The reasonable practical steps to be started before process to collect data or as soon as reasonably practicable after the collection of data.

The Organisation for Economic Cooperation and Development (OECD) advocates the principle for data subject participation. In terms of this principle, the data subjects possess three rights. The first is the right to request that the responsible party confirm whether it holds data belonging to a data subject. The second is the right to correct all the inaccurate information found in the data belonging to a data subject. The third is the right to object to the processing of their data in certain circumstances. (15)

(50)

<u>Question 2</u>

2.1

2.1.1 Section 43 of the Electronic Communications and Transactions Act prescribes the information a webtrader must supply to its website. Generally, the information has to contain the full names and the legal status of the webtrader. If a webtrader is a legal person, the information must contain its registration number, the names of its officer-bearers & its place of registration. In addition, the information should contain the physical address, telephone number, website address and e-mail address of the webtrader, and the physical address at which the trader will receive legal service of documents. Furthermore, the fact that the webtrader's membership of or subscription to any self-regulatory, accreditation or professional body, and the contact details of that body has to appear from the information. Also, the information must detail the any code of conduct to which the webtrader subscribes and how the code may be accessed electronically by the consumer. It has to state the adequate description of the main characteristics of the goods or services offered, to enable a consumer to make an informed decision about the proposed electronic transaction, the full price of the goods/services, including transport costs, taxes and any other fees or costs and the manner of payment, and the terms of agreement, including guarantees, that will apply to the transaction & how those terms may be accessed, stored & reproduced electronically by consumers. Lastly, the information must contain the time when goods will be dispatched/delivered or within which the services will be rendered and the manner in and period within which consumers can access & maintain a full record of the transaction. In this regard, the following must appear from the information:

1. The return, exchange & refund policy of the webtrader,

2. Any alternative dispute-resolution code to which the webtrader subscribes & how that code may be accessed electronically by the consumer.
3. Webtrader's security procedures & privacy policy in respect of payment, payment information & personal information. (10)

2.1.2 Firstly, a webtrader must give consumers the opportunity to review electronic transactions, correct any mistakes in the electronic transactions and withdraw from the electronic transactions. Failure to do so results in the consequences stated in s 43(2) and 20 of the Electronic Communications and Transactions Act. In terms of section 43(2), a consumer is entitled to withdraw from the transaction within 14 days of receiving the goods or services if the webtrader failed to give her or him the prescribed opportunity to review, correct and withdraw. Furthermore, section 20 gives a consumer the right to cancel, retrospectively, the agreement if webtrader fails to give the consumer opportunity to prevent or correct mistakes at the time of the consumer's interaction with the electronic agent.

Secondly, section 43(5) of the Electronic Communications and Transactions Act details the payment procedure to be followed. In terms of this section, a webtrader has to use payment system that is:

- Sufficiently secure with reference to accepted technological standards at the time of the transaction.
- Sufficiently secure with reference to the type of transaction concerned.
- As regards current technology, the following procedures must be met:
    1. A digital certificate from a recognized security provider that authenticates the website.
    2. Encryption technology that encrypts data messages between webtraders and consumers, and webtraders and payment institutions.
    3. The use of usernames and passwords by consumers to gain access to the same webtrader after the initial transaction.
    4. A time-out function in login or transaction pages which automatically logs the user off when there is no activity on the page for a certain period of time.
    5. Offline/off-site storage of payment information where possible.

- A webtrader should secure its payment-security procedures to ensure that they are up to date and that they comply with the requirements of section 43(5).

Thirdly, a webtrader must comply with its normal contractual obligations in terms of applicable legal system. These are indicated in section S 46 of the Electronic Communications and Transactions Act. In terms of this section, a webtrader has to execute consumer's order within 30 days of receiving the order, unless stated otherwise in a contract. Furthermore, section 46(2) gives a consumer the right to cancel an agreement with 7 days' written notice to the webtrader if webtrader fails to execute the order within 30 days. In addition, section 46(3) states that when webtrader becomes aware that the goods or services ordered are unavailable, it shall notify the consumer of that fact and refund, within 30 days of the notification any payment received. (15)

2.2

2.2.1 There are number of principles of e-government. The first is that e-government connotes, as the name indicate, the use of technology for governance. It implies something more that the presence of government in online settings. The second is that e-government encourages the shift from offline society to an information or digital society. Accordingly, brings a about a new kind of citizenry, that is, e-citizens. The latter are the citizens who access the services of the state and partake in the decision-making of the state online. The third is that e-government ought to available and accessible to the e-citizens. Specifically, e-government should lessen or ameliorate the digital divide between government and citizens. The fourth is that e-government is network government or government using modern technologies. In this manner, all government departments work together to deliver efficient and effective services to the e-citizens. The fifth is that e-government is prefers open-source. On the one hand, this alleviates the financial and administrative burden on the state. On the other hand, it mitigates the challenges of accessing e-government services by the e-citizens. The sixth is that e-government promotes collaborative governance. This working-together takes place at all the levels of government. (10)

2.2.2 Government can use a number of tools to effect e-government services. The most essential are the following:

- Effective, efficient and cost effective service delivery.

- Reduced corruption and exploitation.
- Increased citizen e-government participation and interaction.
- Transparency.
- Accountability or answerability.
- Convenient and available e-government information and services.
- Improved customer services.
- Increased access to e-government information and services. (10)

2.3 Online Dispute Resolution refers to a wide variety of alternate dispute resolution processes that take advantage of the availability and increasing development of information and communications technology. It contains a set of dispute resolution processes that allow for the resolution of disputes via online or digital mechanisms, for example, the Internet or some form of technology that allows for virtual communication without requiring the parties to be in contact with each other. In addition, online dispute resolution is a means of dispute settlement whether through conciliation or arbitration. In effect, ICTs are used to facilitate the resolution of disputes between parties. It is similar to offline conciliation and arbitration but the information management and communication tools that are used during the proceedings, and may apply to all or part of the proceedings have an impact on the methods by which the disputes are being solved.

According to the United Nations Commission on International Trade Law (UNCITRAL), Business-to-business and business-to-consumer electronic commerce has rapidly developed over the past decade. This development is, in the main, based on the "exponential diffusion of the Internet, increased broadband access and the rise of mobile commerce throughout the world". Because of this, online dispute resolution is seen as an optional instrument for the resolution of business-to-consumer transactions. Within the context of the UNCITRAL, the latter is referred to as the "Blue Button". For online dispute resolution to be effective, it has to meet certain characteristics. These are that the following:

- Voluntariness – This means that the parties voluntarily elects to participate in the online dispute resolution process and chooses to pursue their claim using this process. Usually, voluntariness gives the parties the choice to withdraw from the process at any given time.

- Informality - The proceedings are generally more relaxed and informal. The process is in an asynchronous manner and the parties have the time to engage and reflect on their respective positions before coming to any agreement.

- Confidentiality – The process is confidential. This rule may be departed with in certain circumstances, for example, in cases where the parties agree otherwise.

- Neutrality – Online dispute resolution is a neutral and impartial process. The basis is to help or assist the parties to arrive at a mutually acceptable settlement.

(50)

[100]