UNIVERSITY OF JOHANNESBURG

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

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

NUMBER OF PAGES: 10 PAGES

INSTRUCTIONS:

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

Question 1

1.1 Generally, crimes are part of society. Traditionally, computers were but another tool to commit crimes. This could happen in three ways. Firstly, computer could be an instrument to perpetrate crimes. Secondly, computers could be a target to attack or carry out cyber-attacks. Thirdly, computers could be storage machinery (zombie) that perverse information related to crime. Conventionally, we now talk of the vibrant concept of "information and communications technology (ICT)". Thus, the focus is on cybercrimes as opposed to the use of computers to commit crimes.

One example to demonstrate this is to study the common crime of theft or furtum. To prove this crime, one has to demonstrate that there was *Contrectatio* (physical touching or handling of a thing), *Rei fraudulosa* (fraud), *Lucri faciendi gratia* (for purposes of gain) and *Ipsius re vel usus eius possessionisve* (depriving owner or possessor of possession). The question that flows from this is whether there is such a thing as the physical touching or handling of, for example, data? Snyman introduced the notion of 'appropriation". He states that the following:

> *"Contrectatio* might have been a satisfactory criterion centuries ago when the economy was relatively primitive and primarily based on agriculture. In today's world with its much more complicated economic structure, it is far better to use the more abstract concept of appropriation to describe the act of theft than the term *contrectatio*, unless one discards the original meaning of the latter term and uses it merely as a technical *erudite-sounding* word to describe the act of theft".

According to Snyman, appropriation means the assumption of control of or over property of another. The gaining control of possession does not necessarily refer to the touching or handling. It simply implies the intention to deprive the owner permanently of the benefits of ownership. Furthermore, in *S v Graham* [1975] 3 All SA 572 (A), the court had to decide whether a payment made by means of a cheque into A's account amounted to theft or not. It stated that the principles of theft are founded on a 'living system'. This system is flexible and adaptable. In addition, this flexibility enables the system to be in touch with current realities and to be able to respond to existing societal conditions. Consequently, the court concluded that money is capable of being stolen even in cases where it is represented by entries in books of accounts, for example, credits. This view was followed by the court in the case of *S v Mintoor* (1996) 1 SASV

514 (K) and *S v Harper and another* (1981) 2 SA 638 (D).

Despite this, there are a number definitions of cybercrimes. Some refer to these crimes as the technological crimes, electronic or e-crimes, computer crimes, internet-related crimes or net crimes. The academic viewpoint is that cybercrimes are any violation of criminal law that involves knowledge of computer technology by the perpetrator, investigator or prosecutor. They involve any crime carried out primarily by means of a computer or the Internet (deleting information without requisite authority, defacing a website, web graffiti) or any form of dishonest conduct associated with the mechanical processing or transmission of information.

However, section 1 of the Electronic Communications and Transactions Act states that cybercrimes are any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them. In terms of section 87, they involve the crime of attempt, aiding and abetting. Also important is Notice 888 of 201249 in Government Gazette No. 35821 which defined cybercrimes as any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them. (20)

1.2

1.2.1 Indeed, the collection and use of Sipho's personal information in this manner amount to the processing of information as envisaged in the Protection of Personal Information Act 4 of 2013 (POPI Act). Specifically, section 1 of the POPI Act defines the term processing in the following manner:

> "Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information".

Therefore, this collection and use falls within the ambit of the POPI Act. The latter regulates the manner of preserving the integrity of personal information and governs the manner of collecting and processing this information. The idea for this is to preserve the sanctity of Mike's personal information.

1.2.2 In the example above, the processing of the personal information

appears to be lawful and have been carried out in a reasonable manner. Specifically, the processing of the personal information in line with the (original) purpose specification (OECD Guidelines), that is, making a decision whether admit Sipho or not. Furthermore, the data subject (Sipho) consented to the processing of the information and which processing is necessary in ensuring that Sipho becomes one of the students enrolled to the LLG Programme.

In addition, the processing of Sipho's personal information is in line with condition or principle for "Purpose Specification". This principle states that data must be collected for a specific purpose, an explicitly defined purpose, and a lawful purpose. This means that a data subject has to know and be aware of the purpose of collection. The requisite knowledge and awareness must exist no later than at the time of collecting the data. In addition, the knowledge may not be vague, uncertain and unlawful. Accordingly, it must relate to the use of data. This use must be restricted only to the achievement of that purpose, or any other purpose that is compatible with the first-mentioned purpose. In situations where data is recorded, the records must then be kept in a manner that conforms or attains the purpose for which the data was initially collected.

Important also is the principle for "Further Processing Limitation". This principle states that personal information must be processed in accordance with the purpose for which the data was initially collected, or must be compatible with the purpose for which the data was initially collected. (10)

1.2.3 Yes, the situation will be completely different. The cardinal principle of our law is that personal information must be processed lawfully and the processing must be in a reasonable manner that does not infringe the privacy of the data subject (s 9(a) and (b) of the POPI Act). This means that such a processing may be made if it is adequate, relevant and not excessive (s 10 of the POPI Act). In determining the aforesaid, section 11 of the POPI Act sets out the principles to be followed. In terms of this section, personal information may be processed if:

- The data subject or competent person where the data subject is a child consents to the processing,
- Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party,
- Processing complies with an obligation imposed by law on the

responsible party,

- Processing protects the legitimate interest of the data subject,
- Processing is necessary for the proper performance of a public law duty by a public body, or
- Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to who the information is supplied.

In addition to this, the collection and use of Sipho's information for advertising purposes amounts to the further processing of his personal information. Therefore, this processing must be in line with the purpose for which the information was initially collected, or must be compatible with the purpose for which the information was initially collected, that is, making the decision regarding whether to admit Sipho to the LLB Programme.

Having examined the facts and the law, it can be said that the use of Sipho's information for advertising purposes is unlawful and unreasonable. This arises not only because Sipho did not consent to the processing, but also because this processing does not meet all the other requirements for the lawful processing of personal information. For example, the responsible party (University of Johannesburg) cannot demonstrate that the processing was necessary to conclude or perform in terms of the contract. The contract it had with Sipho was to the latter to be enrolled as an LLB student. Furthermore, the processing does not meet the conditions set out in section 11 of the POPI Act. (10)

1.3 The exceptions to the general rule that the processing of sensitive information is prohibited are that sensitive data may only be processed if:

- Data subject has explicitly consented.
- Processing relates to data made public by the data subject.
- Processing is carried out by a non-profit-seeking body for:
    1. Political purposes,
    2. Philosophical purposes,
    3. Religious purposes, or
    4. Trade-union purposes.

- The processing is necessary for data controllers to:

    1. Carry out their obligations in the field of employment law,

    2. Protect the important interests of data subjects/those of another person, or

    3. Establish or create legal claims/defend themselves against such claims. (5)

(50)

Question 2

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 electronic 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. (5)

(50)

[100