

IPSP078 - Legal Aspects of Electronic Commerce

Assignment 1: 641343

Nyameko Lisa

31 August 2018



Declaration

I know that plagiarism is to use someone else's work and pass it off as my own.

I know that plagiarism is wrong.

I confirm that this assignment is my own work.

I have acknowledged in the bibliography accompanying the assignment all the sources that I have used.

I have not directly copied without acknowledgement anything from the Internet or from any other source.

I have indicated every quotation and citation in a footnote or bracket linked to that quotation.

I have not allowed anyone else to copy my work and to pass it off as their own work.

I understand that if any unacknowledged copying whatsoever appears in my assignment I will receive zero per cent for the assignment.

I am aware of the UNISA policy on plagiarism and understand that disciplinary proceedings can be instituted against me by UNISA if I contravene this policy.

I indicate my understanding and acceptance of this declaration by entering my name here under:

- Name: **Nyameko Lisa** (Student Number: **7874-909-3**)

NOTE

Please note that footnotes will be denoted as ¹ and will appear at the bottom of the page.

References will be denoted by [1] and will appear at the end of the document.

¹This is a footnote.

1 Question 1 [15]

1.1 List five legal challenges that electronic commerce poses (5).

Electronic commerce poses a number of regulatory and legislative challenges, which as described in [1]–[8], include but are not limited to:

- Contract Laws, Evidence, Validity of Agreements
- Liability, Legal Formalities, Automated Contracts and Agency, in terms of Time, Place, Written, Signatory and Notary Requirements of Contracts
- Consumer Protection, Offer \ Acceptance and Privacy Issues
- Applicable International Guidelines, Laws and Jurisdiction
- Harmonisation of ICT Policies Across Competitive Regional Markets
- Fair Access to the Mechanisms and Infrastructure of Electronic Commerce
- Intellectual Property Rights
- Legislation of Criminal Activities Associated to Electronic Commerce
- Taxation, Banking Laws and Electronic Payments (Cyber Credit and Crypto-Currencies as forms of Legal Tender)

The above considerations were succinctly articulated and categorised into areas of concern requiring serious consideration in e-commerce policy formulation in [9], as the need for confidence in the security and privacy of transactions performed electronically, the need to enhance the information infrastructure for electronic commerce, the need to establish rules that will govern electronic commerce, and the need to bring the opportunities of e-commerce to the entire population.

1.2 Explain the extent to which the Electronic Communication and Transactions Act of 2002 has addressed these challenges (10).

The extent to which the Act addresses some of the challenges mentioned above will be discussed under the following headings:

1.2.1 National e-strategy and electronics transactions policy

As per the provisions of [section 2(1)][1], together with [section 2][2], the objectives of the Act are to enable and facilitate electronic communications and transaction in the public interest.

As per the provisions of [section 5(3)][1], together with [section 3][2], national e-Strategy and policy framework has been well articulated in that strict timelines have been laid out the implementation, submission and acceptance by Parliament thereof. The Act also permits liaison and consultation with public and private bodies in this endeavour.

It is unfortunate indeed to elaborate on these severe shortcomings of the ECT Act [1] and the failures of Government. Initially the Act made explicit provisions that mandated the Ministry to promote universal access particularly to historically previously disadvantaged persons and communities, [section 6 & 7][1]. These provisions were subsequently deleted in the amendment bill [section 4][2].

The ECT Act [1] has also failed to support SMMEs in that explicit provisions outlined in the support of programmes and infrastructure promoting the utilisation and development of electronic commerce by SMMEs [section 9][1], were subsequently removed in the amendment bill [section 6][2].

1.2.2 Facilitation of electronic transactions

The ECT Act [1] makes provisions for the legal recognition of data messages, formation and validity of agreements and their time and place, and the offer and acceptance of agreements, as per [sections 11, 22-24 & 26][1] and [section 8][2], respectively. Moreover as per [sections 12, 13 & 14][1], the Act makes provision for the recognition of electronic data messages as legal agreements or contracts, in outlining the requirements data messages need satisfy in terms of being in writing, signatures and originality, respectively.

As per the provisions of [sections 15-20][1], together with [section 9][2], information in the form of an electronic data message is admissible in legal proceedings and must be given due evidential weight.

1.2.3 Consumer protection and protection of personal information

As per the provisions of [sections 42-48 & 50-51][1] together with [sections 21-25 & 26][2], the ECT Act [1] has gone to great lengths to articulate in meticulous detail both ‘consumer protection’ and ‘protection of personal information’ respectively.

Regarding consumer protection, the provisions are more than adequate in terms of describing: scope of applicability [section 42][1], required information [section 43][1], cooling-off periods [section 44][1], unsolicited goods, services or communications [section 45][1], roles and performers [section 46][1], applicability of protection irrespective of foreign law and non-exclusion [section 47 & 48][1].

Regarding the protection of personal information, again the provisions are more than adequate in terms of describing the scope of protection [section 50][1], the principles for electronically collecting personal information, together with those provisions stipulated in [10].

1.2.4 Domain name authority and administration

As per the provisions of [chapter X][1], together with [sections 28-35][2], challenges with respect to the establishment and incorporation of a “.za” domain name authority are more than adequately addressed. Moreover together with [11], the ECT Act [1] makes provisions for alternative mechanisms for the resolution of disputes arising in the “.za” domain name space.

1.2.5 Limitation of liability of service providers and cyber crime

As per the provisions of the ECT Act [1], a service provider is not liable for damages arising from said service provider for providing access to or for operating facilities as a ‘*mere conduit*’ [section 73][1] together with [section 38][2], ‘*caching purposes*’ [section 74][1] together with [section 39][2] and ‘*hosting services*’ [section 75][1]. Moreover the Act explicitly excludes service providers’ obligation from monitoring data, as per [section 78][1].

As per [chapter XII][1], together with [sections 43-45][2], the Act makes for adequate provision in terms of “cyber inspectors”. [Section 86][1] together with [section 48][2] addresses issues related to unauthorised access to, interception of or interference with data; [section 87][1] together with [section 49][2] addresses issues pertaining to computer related extortion, fraud and forgery; [section 88][1] together with [section 50][2] address issues pertaining to (attempted) aiding and abetting; lastly [section 89][1] together with

[section 51][2] pertains to the consequences and penalties that a person convicted of a cyber offence is liable to.

1.2.6 General provisions as they apply to jurisdiction of courts and saving of common law

As per the provisions of [section 3][1], the Act cannot be interpreted in any way such as to exclude the application of existing statutory or common law and must necessarily take them into account as per the provisions of [section 3(d) & section 10(2)(b)(iii-iv)][2]. Those sections also stipulate that the Act must adhere to international best practice and conform to the laws and guidelines of other jurisdictions and international bodies. Finally, [chapter XIV][1], together with [section 52-55][2] addresses issues pertaining to jurisdiction of the courts of the Republic matters in trying offences in terms of the ECT Act.

2 Compare and contrast the challenges addressed in the ECT Act with the following [10]:

2.1 The UNCITRAL Model Law on Electronic Commerce of 1996 (5)

Challenges related to the facilitation of electronic transactions are handled in a very similar manner in [parts 1 & 2][1] '*legal requirements for data messages*' and '*communication of data messages*', and in [chapters II and III][12] '*application of legal requirements to data messages*' and '*communication of data messages*' respectively.

Where there are discrepancies however is in the challenges posed by matters related to consumer protection, protection of personal information, domain name administration, limitation of liability in respect of service providers, and cyber crime, to name but a few. These challenges whilst addressed in the ECT Act [1], are not handled at all in the UNCITRAL Model Law [12].

Lastly where the ECT Act [1] has clear shortcomings, are challenges posed by electronics commerce with regards to the carriage of goods [articles 16 & 17][12], which is not handled at all within the ECT Act [1].

2.2 The SADC Model Law on Electronic Transactions and Electronic Commerce of 2012. In your answer briefly explain what impact the SADC Model will have on the South African legislation and those of neighbouring countries (5)

The provisions of the ECT Act [1] are almost identically aligned with the provisions of the SADC Model Law [13]. From the SADC Model Law, part 1 - '*general enabling provisions*', part 2 - '*electronic transactions*', part 3 - '*electronic commerce*', part 4 - '*consumer protection*' and part v - '*service providers*'. The SADC Model however, makes no references to domain name authorities and cyber law to name but a few discrepancies.

The impact of the SADC Model, will be the harmonisation of regional ICT communication, transaction and commerce policy. Without the SADC Model as an overarching and guiding template, neighbouring countries may potentially develop contradictory regulatory frameworks that impede regional electronic commerce.

References

- [1] Electronic Communications and Transactions Act No. 25, 2002.
- [2] Electronic Communications and Transactions Amendment Bill, 2012.

- [3] Eiselen, “E-Commerce,” in *Information and Communications Technology Law*, D. van der Merwe, Ed., Second, 2016, 149-181 and 195-220.
- [4] Papadopoulos, “An introduction to cyberlaw,” in *Cyberlaw @ SA III: The law of the Internet*, Papadopoulos and Snail, Eds., Third, 2012, 1–8.
- [5] Buys, “Towards an electronics commerce policy for south africa,” in *Cyberlaw: The Law of the Internet @ SA*, First, 2000, 97–112.
- [6] Pistorius, “Copyright Law and IT,” in *Information and Communications Technology Law*, D. van der Merwe, Ed., Second, 2016, 267-270 and 292-362.
- [7] B. Hamann and S. Papadopoulos, “Direct marketing and spam via electronic communications: An analysis of the regulatory framework in south africa,” *De Jure*, vol. 47 (1), 42–62, 2014.
- [8] Pistorius, “Domain Names and Infringement of Trade Marks on the Internet,” in *Information and Communications Technology Law*, D. van der Merwe, Ed., Second, 2016, 221–265.
- [9] A green paper on electronic commerce for south africa, Department of Communcations, 2000.
- [10] Protection of Personal Information Act No. 4, 2013.
- [11] Electronic Communications and Transactions Act No. 25: Alternative Dispute Resolution Regulations, 2006.
- [12] Model Law on Electronic Commerce with Guide to Enactment, United Nations Commission on International Trade Law, 1996.
- [13] Electronic Transactions and Electronic Commerce: SADC Model Law, Harmonization of ICT Policies in Sub-Saharan Africa, 2013.