The Influence of the ECT Act on a Typical Computing Curriculum

Andries Barnard

Laurette Pretorius

Lucas Venter

Abstract

Recent technological advances have led to the emergence of new technologies, frameworks and methodologies in the field of computing, the regulation of which are governed by scientific principles. Examples include the Internet, global connectivity and mobile agent technology, collectively referred to as cyberspace. Regulating human interaction with cyberspace has become one of the great challenges of the information age – a challenge in which legislation plays a central role.

At present the regulation of human interaction with cyberspace by means of legislation, is awarded prominence on a global level by governments. In this regard the computing instructor plays a central and multi-faceted role. It is within this context that we consider what influence the new South African Electronic Communications and Transactions (ECT) Act (Act No. 25, 2002) may have on a typical computing curriculum.

Keywords

South Africa, ECT Act, Computing Curriculum

1. Introduction

Advances during the past decade have led to the emergence of, among others, new technologies, frameworks and methodologies in the field of computing. Examples include the Internet, global connectivity and mobile agent technology, collectively referred to as cyberspace. Regulating cyberspace has become one of the great challenges of the information age, a challenge in which the computing professional plays a central and multi-faceted role. Therefore, computing professionals have to, in fulfilling their role in society, take into consideration the fact that cyberspace is populated by both humans and artificial entities.

At present the regulation of cyberspace by means of legislation is awarded prominence on a global level by governments. It is within this context that we consider what impact the new South African Electronic Communications and Transactions (ECT) Act (Act No. 25, 2002) could have on a typical computing curriculum. In section 2 we give a brief overview of the Act and discuss some shortcomings. More specifically, we note that the Act deals in particular with Internet related activities. These activities range from providing a mere description of data messages, to complex measures (including various security considerations) relating to and attempting to realise the governance of e-commerce transactions in South Africa. Section 3 contains a discussion of the impact of the Act on three subject areas mentioned in the ACM/IEEE computing curriculum (Computing Curricula ..., 2001). Although the discussion is not exhaustive, it demonstrates how the Act could impact on other aspects of this curriculum.

2. The Electronic Communications and Transactions Act, 25 of 2002

The ECT Act is considered to be of great strategic importance for the whole continent of Africa, as is argued in (Van der Merwe, Pretorius and Barnard, 2004). Because South Africa has been one of the first African countries to adopt this type of legislation, it is possible that the Act might serve as a model for the entire Sub-Saharan African region. The purpose of the Act, as stated in its preamble (Act No. 25; 2002), is:

- *"to provide for the facilitation and regulation of electronic communications and transactions;*
- *to provide for development of a national e-strategy for the Republic;*
- *to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs (Small, Medium and Micro Enterprises);*
- *to provide for human resource development in electronic transactions;*
- *to prevent abuse of information systems;*
- *to encourage the use of e-government services; and*
- *to provide for matters connected therewith."*

In addressing this purpose, the Act covers, amongst others, the following topics (dealt with in individual chapters of the Act):

- Electronic transactions: chapter III;
- E-government services: chapter IV;
- Cryptography providers: chapter V;
- Authentication service providers: chapter VI;
- Consumer protection: chapter VII;
- Protection of personal information: chapter VIII ;
- Protection of critical databases: chapter IX;
- Domain name authority and administration: chapter X;
- Limitation of liability of service providers: chapter XI;
- Cyber inspectors: chapter XII;
- Cyber crime: chapter XIII.

Sections 13 to 20 of chapter III that deal with electronic transactions have overcome one of the biggest obstacles regarding electronic commerce without paper embodiments, namely the question of proof of the contents of electronic documents. By affording data messages admissibility as evidence, the court bypasses the paper trail that has characterised especially civil litigation in the past. A data message is defined in section 1 of the Act as: *"data generated, sent, received or stored by electronic means, and includes a) voice, where the voice is used in an automated transaction and b) a stored record"*. Van der Merwe *et al.* (2004) note that it remains to be seen, however, how much weight a judge or magistrate will afford a document that is only available in electronic format. Section 15(4) provides that a data message created *"in the ordinary course of business"* presents rebuttable proof of its contents, thus transferring the onus to produce evidence of a lack of reliability on the party aggrieved by the admission of the electronic document.

Furthermore, section 20 of the Act should have implications for the use of artificial entities. In particular, chapter I, section 1 of the Act defines an electronic agent as *"a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part in an automated transaction"*. This section provides for an agreement, or *contract* in a commercial sense, to be created by an artificial entity, in this case an electronic agent. This extends the class of entities that can be involved in legal situation.

The recent importance attached to the actions of artificial entities (software agents) in cyberspace (Barnard, Cloete and Pretorius, 2004), raises the question of what would happen if both parties made extensive use of what the Act refers to as electronic agents. In such an event much of the consumer protection built into chapter III, section 20 seems to fall away because natural persons are reduced to peripherals while the electronic agents (code, architecture, software agent, etc.) are responsible for effecting a transaction (Van der Merwe *et al.*, 2004).

Furthermore, the South African Police Services already have a Computer Crime Unit. Buys and Cronjé (2004) argue that the force of cyber inspectors envisioned by the Act, is in conflict with this existing law enforcement agency. They state that the appointment of a force of cyber inspectors *"that have wide-ranging, invasive powers, yet do not have the experience and additional resources of the SAPS, is an unwarranted extension of the powers of the Department of Communications"* (Buys and Cronjé, 2004:335-336). However, many of the officials required to carry out important functions in terms of the Act still have to be appointed, and the necessary infrastructure must be put in place. For example, chapter IV of the Act provides for an Authentication Service Provider that will include an Accreditation Authority, both of whom are necessary to certify the authenticity of an advanced electronic signature. Similarly, the cyber inspectors provided for in Chapter XII have not yet been appointed. This points to a potential shortcoming of the current provisions of the Act.

Lessig (1999) describes four modalities that impact on the regulation of modern society, viz. norms, law, market forces and computer code (architecture). He argues that in the absence of strong influences by the first three modalities to regulate modern society, increasing prominence may be awarded to the use of computer code (architecture) to effect such regulation. Hence, when the Department of Communications put these measures in place and appoint the relevant officials, the Department would have to avoid possible conflict with existing law enforcement agencies, such as the SAPS Computer Crime Unit. The alternative may well lead to a greater dependence on computer code (architecture) for regulation. In the above example, the guarantee of authenticity may simply be left to computer code (architecture). This may well lead to increased dominance by certain software developers.

An initiative in providing the necessary infrastructure to enforce this legislation was reported on January 12, 2004 (SABC News, 2004). In particular, the *"US Secret Service has donated 22 specialised forensic computers to help combat cyber crime in this country. They are valued at more than a million rand"*. Training is envisioned to take place in two phases. Firstly members of the SAPS Computer Crime Unit will be trained, followed by legal practitioners including judges and prosecutors.

In concluding this section on the ECT Act we briefly note the first conviction in terms of this act. Two perpetrators, Michael Bafatakis and Andrew Stokes, gained illegal access to a South African mobile telecommunications operator, Vodacom, and downloaded personal information of Vodacom clients. They attempted to blackmail Vodacom for an amount of ten million rand not to disclose this information. The conviction (November 2003) of the two perpetrators was the first in terms of this new act (Sake Rapport, 2003), regarding the contravention of sections 86 and 87 of the Act.

3. A Typical Computing Curriculum

For the purposes of this paper we use the proposed ACM/IEEE Computing Curricula (Computing Curricula ..., 2001) as an example of a typical computing curriculum. Both the IEEE and ACM endorsed the curricula recommendation of this report. Many textbooks currently in use at universities worldwide, and certainly at UNISA, are based on the guidelines given in this report. Hence it is clear that this report has a large impact, directly and indirectly, on curricula at many universities. A good example of this is the recent trend to include sections on social and professional issues (Computing Curricula …, 2001: Subject area 12) in many computing textbooks.

This body of knowledge is organised into fourteen disciplinary subfields or subject areas. We consider the impact of the Act on a selected number of subject areas of this curriculum. In the context of the previously stated purpose of the Act and the structure of the CS body of knowledge (Computing Curricula ..., 2001) we are of the opinion that the teaching of the following three subject areas may, and should, take cognisance of the contents of the Act:

- Net-Centric Computing,
- Information Management, and
- Social and Professional Issues.

The reader is referred to Appendix A of (Computing Curricula …, 2001) for more information concerning these subject areas.

3.1 Net-Centric Computing

In the above-mentioned appendix the contents of this area are summarised as follows: *"Recent advances in computer and telecommunications networking, particularly those based on TCP/IP, have increased the importance of networking technologies in the computing discipline. Net-centric computing covers a range of sub-specialties including: computer communication network concepts and protocols, multimedia systems, Web standards and technologies, network security, wireless and mobile computing, and distributed systems."*

In this section, we restrict our discussion to three specific topics of the Act that deal with information security. Chapter III of the act makes provision for the facilitation of electronic transactions. In particular, it defines an electronic document and specifies how to deal with these documents. Chapters V and VI of the Act deal with cryptography and authentication service providers, and chapter XII makes provision for the appointment of Cyber Inspectors. We show how these chapters impact on the teaching of Information Security. Of special interest are the following topics covered in subject area NC3: Network security (Computing Curricula ..., 2001):

- Fundamentals of cryptography
- Secret-key algorithms
- Public-key algorithms
- Authentication protocols
- Digital signatures.

3.1.1 Electronic Transactions and Documents

The act in effect affords a data message, discussed in section 2 above, the same status as any other legal document, if it complies with two requirements. The document must be *signed* with an advanced electronic signature, and it must be retained (stored) in such a way that (see section 16 of the Act):

- the information contained in the document is accessible;

- it can be demonstrated that the stored message accurately represents the information contained in the original document;
- the origin and destination, as well as the date and time sent and received, can be determined.

The advanced electronic signature mentioned by the Act is simply a standard electronic signature, which is issued by a registered authentication service provider. The signature should be uniquely linked to a specific user who must be identified on a face-to-face basis, must be capable of identifying that user, and must be created by means under the sole control of that user. The signature should also be linked to a specific data message and should be capable of detecting any subsequent changes to the contents of the message. These requirements are fairly standard, and can to a large extent be provided by using hash functions and public key encryption techniques, such as described in any standard textbook, for example (Pfleeger 1997: 96-98). This can be illustrated by learning objective 4 of topic NC3 (Network security), which states *"Summarize common authentication protocols."* (Computing Curricula …, 2001).

A problem arises when the storage of data messages is considered. The Act does not specify that the message must be stored in its original format; rather, the Act specifies that the information contained in the document must be accurately represented. Current authentication techniques can only ensure the authenticity of a document if it is stored in its original format (Pfleeger 1997: 97). Research in this area might lead to an advanced degree.

3.1.2 Cryptography and Authentication Service Providers

The Act requires that all providers (not users) of encryption services or products must be registered. It defines an encryption product as any (software) product that contains any form of encryption. This implies for instance that Linux, which is freeware, is classified as an encryption product. Hence versions of Linux distributed through download sites become illegal. Commercial providers of products containing Linux would have to register as a cryptography provider, even though their product might not be available in South Africa, but is simply used by some person in this country. This subtlety of the Act would have to be emphasised in courses where any aspect of cryptography is taught.

Courses on cryptography would also have to deal with ethical issues. For instance, a cryptography provider can be required by law to disclose all information regarding services provided to a specific client. The provider would have to consider ethical issues when deciding how much information he/she will store. This issue is related to SP7: Privacy and civil liberties, mentioned in section 3.3 of this paper.

The act also creates the possibility to register authentication service providers, whose main task will be to provide advanced electronic signatures for data document authentication. This registration is not compulsory, as in the case of cryptography providers. The reason for this might be that most known effective authentication techniques are based on cryptography, and hence that these providers will have to register as such. Typically, these services will be provided by computing professionals and therefore these issues need to be adequately addressed in a computing curriculum.

3.1.3 Cyber Inspectors

The activities of cryptography and authentication service providers will be monitored by Cyber Inspectors. These inspectors will also have the authority to monitor and inspect any web site or activity on an information system in the public domain. They would have to have the skill to determine whether a cryptographic or authentication service is provided. Once this is established, they must also have the ability to determine whether the service rendered is in compliance with the provisions of the Act. Highly specialized training programs would have to be developed to train these inspectors.

3.1.4 Information Management

In Appendix A of (Computing Curricula ..., 2001) the contents of this area are summarised as follows: *"Information Management (IM) plays a critical role in almost all areas where computers are used. This area includes the capture, digitization, representation, organization, transformation, and presentation of information; algorithms for efficient and effective access and updating of stored information, data modeling and abstraction, and physical file storage techniques. It also encompasses information security, privacy, integrity, and protection in a shared environment."*

Chapter VII of the Act deals with consumer protection. In particular, section 43 deals with information to be provided by service and goods providers making use of electronic means. This information to be provided to potential customers include, amongst others:

- Code of conduct to which the supplier subscribes (section 43(1)(e)).
- Any terms of agreement, including any guarantees, that will apply to the transaction, and how those terms may be accessed, stored and reproduced electronically by consumers (section 43(1)(k)).
- Security procedures and privacy policies of that supplier in respect of payment, payment information and personal information (section 43(1)(p)).

It is therefore important that the computing instructor should equip the computing student with the technical knowledge and skills to adhere to the requirements of these and other stipulations of this chapter of the Act. This is in accordance with learning objective 4 of topic IM1 (Information models and systems) that reads: *"Describe several technical solutions to the problems related to information privacy, integrity, security, and preservation"* (Computing Curricula ..., 2001).

Chapter VIII of the Act deals with personal information and privacy protection. Section 51 describes the principles for electronically requesting, collecting, collating, processing and storing of personal information. Learning objective 3 of topic IM1 (Information models and systems) reads *"[c]ritique/defend a small- to medium-size information application with regard to its satisfying real user information needs"* (Computing Curricula ..., 2001).

The Act defines critical data as *"information which, if compromised, may pose a risk to the Republic's national security or the economic or social well being of its citizens"* (Act No. 25, 2002, chapter 1; Deloitte and Touche, 2002). Chapter IX of the Act makes provision for the protection of critical databases. In particular, sections 52 through 55 of the Act deal with the scope of protection, identification, registration, and management of critical data and databases and will account for the protection of critical data. Buys and Cronjé (2004:173) states that the Act contains universally accepted data protection principles setting out how personal information may be collected and used, and note that selective subscription to the Act is not permissible. We therefore consider the adequate coverage of the following topics suggested by (Computing Curricula ..., 2001) to be of crucial importance:

- IM1: Information models and systems;
- IM2: Database systems;
- IM3: Data modelling;
- IM4: Relational databases;
- IM6: Relational database design;
- IM7: Transaction processing;
- IM8: Distributed databases;
- IM9: Physical database design; and
- IM11: Information storage and retrieval.

We also propose that the study of Chapter IX of the Act, as well as its interpretation, and an associated assessment should be included in the study material for and teaching of information management (IM).

We further note that there are issues in this section of the Act that have close links to certain personal privacy issues that are also reflected in the subject area Social and Professional issues of (Computing Curricula …, 2001). These similarities are echoed by Buys and Cronjé (2004, p.172) who state that *"[d]ata protection can factually be regarded as forming part of information privacy"*.

3.2 Social and Professional Issues

Appendix A of (Computing Curricula …, 2001) justifies the contents of this area as follows: *"Undergraduates also need to understand the basic cultural, social, legal, and ethical issues inherent in the discipline of computing. They should understand where the discipline has been, where it is, and where it is heading. They should also understand their individual roles in this process, as well as appreciate the philosophical questions, technical problems, and aesthetic values that play an important part in the development of the discipline. … [S]tudents need to be aware of the basic legal rights of software and hardware vendors and users, and they also need to appreciate the ethical values that are the basis for those rights. Future practitioners must understand the responsibility that they will bear, and the possible consequences of failure."* (Tucker as quoted in (Computing Curricula …, 2001))

It is therefore clear that the computing professional should acquire knowledge and skills regarding the social and ethical issues in computing. A closer look at the subject area, Social and Professional Issues (SP) of (Computing Curricula …, 2001), reveals that the following topics may be linked to the contents of the law in general and/or the ECT Act in particular:

- SP2: Social context of computing;
- SP4: Professional and ethical responsibilities;
- SP5: Risks and liabilities of computer-based systems;
- SP6: Intellectual property;
- SP7: Privacy and civil liberties, and
- SP8: Computer crime.

If we agree that our professional and ethical responsibilities also include the legal systems in place in society, then SP4 should address those laws that regulate various aspects of cyberspace and the computing profession. In the South African case, the ECT Act will play a significant role in regulating conduct and activities in the field of computing, particularly with regard to the Internet. The computing instructor must therefore include pertinent aspects of the Act within this framework.

Chapter XI of the Act deals with the limitation of liability of service providers, that is, persons who provide information system services. It concerns service providers who act as mere conduits, perform caching (automatic creation of temporary copies of electronic data for quick access) or hosting (renting of space to users who provide their own content). Topic SP5 makes provision for including such material in the computing curriculum.

Chapter VII deals with consumer protection, unsolicited electronic communications (spam) and consumer protection for online card payments, topics that are suitable for inclusion into material regarding SP7: Privacy and civil liberties. For example, learning objective 2 of SP7 illustrates this: *"Describe computer-based threats to privacy."*

Chapter VIII, sections 50 (Scope and protection of personal information) and 51 (Principals for electronically collecting personal information) address the protection of personal information. Computing professionals involved in any application that involve so-called electronic transactions should be aware of this chapter of the Act, and also of the fact that the accurate definition of *"electronic transaction"* is still awaited. *"One of the most urgent issues to address, either by Parliament or the courts, will be the definition of electronic transaction."* (Buys and Cronjé, 2004:160).

While making provision for cyber inspectors, who have the power to *"inspect, search and seize"* (section 82), the final chapter (XIII) of the Act deals with cyber crime. Section 86 concerns unauthorised access to, interception of or interference with data (including hacking, cracking and denial-of-service), section 87 addresses computer-related extortion, fraud and forgery and section 88 refers to attempt, and aiding and abetting cyber crime. Topic SP8 of the typical curriculum under consideration makes provision for including issues concerning computer crime. Future computing professionals should take special cognisance of the fact that, according to (Buys and Cronjé, 2004:323):

- a computer can be involved in computer crime as the *object* of the crime, e.g. as victim where unauthorised access and denial-of-service attack is launched against it;
- a computer can be used as *instrument* (tool) in computer crime; and
- a computer can be incidental to an offence, e.g. where it is used to store records of illegal activities.

This is in accordance with learning objective 1 that reads *"Outline the technical basis of viruses and denial-of-service attacks."*

4. Conclusion

"Although technical issues are obviously central to any computing curriculum, they do not by themselves constitute a complete educational program in the field. Students must also develop an understanding of the social and professional context in which computing is done." (Computing Curricula …, 2001).

This quote supports the following concluding perspective:

We considered the impact of the ECT Act on a typical computing curriculum as proposed by the ACM/IEEE. We have seen that in order to address the various aspects of the Act we need to incorporate the fundamental subject areas of this curriculum into our educational programs. The Act, in fact, provides a social context within which we can teach these fundamental aspects.

The ECT Act is but one way in which society expresses its social needs with regard to the regulation of cyberspace. There are also other ways for society to articulate such needs, for example, cultural, normative, moral etc. Each of these impacts on the context within which we may teach the fundamental subject areas of our typical curriculum in its own way. We contend that by teaching universal technical subject content within a localized context the computing professional of the future will be better equipped to face the increasing challenges of the information age.

References

Act No. 25 (2002), The South African Electronic Communications and Transactions Act.

Barnard, A, E Cloete & L Pretorius 2004. A Framework for Performing Security and Ethical Analyses in Agent Computing. *Challenges for the Citizen of the Information Society: Proceedings of the seventh International ETHICOMP conference.* Syros, Greece. In TW Bynum, N Pouloudi, S Rogerson & T Spyrou (eds.) pp. 81 - 93.

Buys, R & F Cronjé 2004. Cyberlaw@SAII. *The Law of the Internet in South Africa*. Pretoria: Van Schaik.

Computing Curricula 2001 – Final Draft (December 15, 2001). http://www.computer.org/education/cc2001/final/index.htm, accessed on 30.04.2004.

Deloitte and Touche Legal 2002. Synopsis of the electronic Communications & Transactions Act

http://www.saica.co.za/documents/Synopsis.pdf, accessed on 30-04-2004.

Lessig, L 1999. *Code: and other laws of cyberspace*. New York: Basic Books.

Pfleeger, CP 1997. *Security in Computing*. Second edition. Upper Saddle River, NJ: Prentice-Hall.

SABC News 2004. US Secret Service Donates 'Crime Fighting' Computers http://www.sabcnews.com/world/north_america/0,2172,71878,00.html accessed on 13.01.2004.

Sake Rapport 2003. Krakers Ry aan die Pen, November 23, pp. 7.

Van der Merwe, DP, L Pretorius & A Barnard 2004. Cyberethics and the South African Electronic Communications and Transactions Act; *Challenges for the Citizen of the Information Society: Proceedings of the Seventh International ETHICOMP Conference*; Syros, Greece. In TW Bynum, N Pouloudi, S Rogerson & T Spyrou (eds.) pp. 860 - 870.

Authors' Contact Details

Andries Barnard (**barnaa@unisa.ac.za**)

Laurette Pretorius (**pretol@unisa.ac.za**)

Lucas Venter (**ventelml@unisa.ac.za**)

School of Computing
University of South Africa, Pretoria, South Africa