LEARNING
~~STUDY~~ UNIT. 01

Cyberlaw@SA III

The law of the internet in South Africa

THIRD EDITION

Sylvia Papadopoulos
Sizwe Snail
(EDITORS)

Van Schaik
PUBLISHERS

346

347
347
347
350
350
350

352

CHAPTER 1

An introduction to cyberlaw

Sylvia Papadopoulos

1.1 INTRODUCTION

There is still some debate as to whether or not society has traversed the frontiers of an industrial society to an information society. Although there is no clear definition of an "information society", it has been described as a society in which information becomes a core economic, cultural and social resource. This debate stems from the fact that almost anything we do is intimately connected to information creation, retrieval, processing or management.[1] Our present relationship with knowledge is very important and has led people to speak in terms of a "knowledge economy" (Rooney, Hearn & Ninan 2005: 5). More specifically, the information society has created and facilitated electronic commerce (e-commerce) whereby businesses and consumers conduct the majority of their every-day transactions via the internet (Fitzgerald, Middleton, Lim & Beale 2007: 13). Therefore, according to the US Department of Commerce, "[the] Internet is both an effect and a cause of the new economy. It is in part, a product of the powerful technological and economic changes that are shaping a new epoch of economic experience."[2]

1.1.1 What is the internet?

The internet is at the heart of this growing information society or knowledge economy, and its key feature is that its core communication infrastructure is seen to be "neutral", with the "intelligence" applied at the "ends", i.e. the so-called end-to-end (E2E) design principle.[3] Thus the idea of "net neutrality" has been a topic of heated debate, spurred on by the fact that there is a need to ensure that the free flow of information across the internet is not undermined by attempts to regulate the core of the internet by differentiating the speed at which different types of content are communicated (Fitzgerald *et al.* 2007: 2).

The internet has its origins in the US military and the Network Information Centre (NIC) of the Stanford Research Institute in the 1960s. Through

1 The World Summit and the Information Society (WSIS)

2 US Department of Commerce Report, *Digital economy* 2000 (See website address in bibliography).

3 This means that communication pathways (i.e. the lines that connect) are neutral and the intelligence in the form of applications, design and customisation is added at the ends, probably by the end-user. According to Lessig (2002), the internet is divided into four layers: physical, transport, application and content. The end-to-end network design proposes that the intelligence be added at a layer closer to the end user in order to avoid control or regulation at a lower level, allowing the network to be utilised by anyone for the broadest possible range of activities. See also Fitzgerald *et al.* (2007: 4).

the activities of various academic institutions it grew throughout the 1970s and 1980s, but it was not until the mid-1990s that the world realised its potential and its use exploded, growing at a phenomenal pace.[4] At the same time developments in telegraph, telephone, radio and computer technology set the stage for an incredible integration of capabilities. The internet therefore has "at the same time a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location" (*http://www.isoc.org/internet/history/brief.shtml*).

The question that may well be asked is: What is the internet exactly? The internet is an interconnected system of networks that connects computers around the world through a software protocol known as TCP/IP.[5] The word internet refers to an "international network" of computers that can communicate with one another through the use of packet switching, a digital communications method. Packet switching was best described in the case of *In re DoubleClick Privacy Litigation*:[6]

> Packet switching works as follows. The computer wishing to send a document ("originating computer"), such as a music file or digital image, cuts the document up into many small "packets" of information. Each packet contains the Internet Protocol (IP) address of the destination Web site, a small portion of data from the original document, and an indication of the data's place in the original document. The originating computer then sends all of the packets through its local network to an external "router". A router is a device that contains continuously updated directories of Internet addresses called "routing tables". The router takes each packet from the original document and sends it to the next available router in the direction of the destination Web site. Because each router is connected to many other routers and because the connection between any two given routers may be congested with traffic at a given moment, packets from the same document are often sent to different routers. Each of these routers, in turn, repeats this process, forwarding each packet it receives to the next available router in the direction of the destination Web site. Collectively, this process is called "dynamic routing".
>
> The result is that packets of information from the originating computer may take entirely different routes over the Internet (i.e. traveling over different routers and cables) to their ultimate destination. Obviously, the packets arrive out of their original order because some have been forced to take much longer or slower routes between the originating and destination computers. However, because each packet contains code that identifies its place in the original document, the destination computer is able to reassemble the original document from the disorganized packets. At that point, the destination computer sends a message back to the originating computer either reporting that it received the full message, or requesting that the originating computer re-send any packets that never arrived. This entire process typically occurs in a matter of seconds.

An end-user will normally connect to the internet through an Internet Service Provider (ISP) who will operate servers that act as storage for the uploaded material. ISPs are often referred to as the gateway to the internet.[7]

1.1.2 What is the difference between the internet and the world wide web?

The internet is the physical infrastructure consisting of servers, computers, fibre-optic cables and routers

4 The internet had its origins in 1969 as an experimental project of the Advanced Research Project Agency (ARPA) and was called ARPANET. This network linked computers and computer networks owned by military, defence contractors and university laboratories conducting defence-related research. The research later allowed researchers to access and use powerful supercomputers located at a few universities and laboratories. From the beginning the network was designed to be a decentralised, self-maintaining series of links between computers and computer networks capable of rapidly transmitting communications without direct human involvement or control, and with the automatic ability to re-route communications if one or more individual links was damaged or unavailable. In other words, it was designed to allow vital research to continue even if a portion of the network was damaged, for example in a war. *American Civil Liberties Union v Reno*.

5 Section 1 of the Electronic Communications and Transactions Act 25 of 2002 (the ECT Act). TCP stands for Transmission Control Protocol and IP for Internet Protocol.

6 *In re DoubleClick Privacy Litigation* (See website address in bibliography).

7 *Dow Jones & Company, Inc. v Gutnick* 56 at 16. See also Fitzgerald *et al.* (2007: 5).

through which data is shared. The world wide web (the "web" or "www")[8] is the data, an immense collection of documents, texts, visual images, audio clips, etc. Servers store this data and make it available through the TCP/IP software protocol. Each document, image or clip has a unique Universal Resource Locator (URL) that identifies their physical location in the internet's infrastructure, and users access them by sending request messages, containing the URL, to the servers that store the documents. When the server receives a user's request, it prepares the document and transmits the information back to the user.[9]

1.1.3 What is internet law, cyberlaw or ICT law?

We live in what has been termed "a quicksilver technological environment", and regardless of perceived ethical or enforcement limitations, laws have become increasingly significant, whether in the enforcement of copyright law regarding the downloading of MP3-formatted songs through file sharing technologies or in the application of the general principles of contract law to online contracts. National law may be seen to have limits, which is why some will argue that technology can be just as powerful as the law in constraining or regulating digital activity (Fitzgerald *et al.* 2007: 1–2).

In the US and Australia academics have been teaching courses on computers and the law for over 30 years (Fitzgerald *et al.* 2007: 2), with South Africa not far behind (e.g. Van der Merwe 2008; Hofman, Johnston, Handa & Morgan 1999; Buys & Cronjé 2004).

The initial approach to the subject was therefore to look at how a legal system was and should be responding to the increasing use of computers and the internet in social and economic life. Many courses and publications went under the title of "Cyberlaw" – the law relating to cyberspace or "Internet law". However, the work in this subject area covers a very broad range of topics, including digital intellectual property, e-commerce, privacy and data protection, freedom of expression and content regulation, cybercrime, electronic or digital evidence, jurisdiction and the regulation of the telecommunication infrastructure. Therefore the terms "cyberlaw" or "internet law" perhaps do not adequately capture the scope of the subject area. There is also the difficulty of settling on a precise title for the subject area, which stems from the fact that there is substantial convergence between the initially separate fields of computers, telecommunication, publishing and broadcasting law.[10] Many of the terms may either invite confusion with other older established existing fields of law or be too narrow to encompass all the aspects of this body of law. Information and communication technology law as suggested by Van der Merwe (2008) seems to be a good compromise. However, for the sake of consistency, in this publication we will continue to use the term cyberlaw and hope that the reader will give it its widest possible interpretation.

The latter approach to the subject is to study the dynamic, substantive and growing body of law so that we can improve, adapt, meaningfully apply the law and keep up with technological advances. There is a growing realisation and awareness that this area of the law cannot be relegated or ignored as a few isolated and obscure legal provisions for a few computer experts and fringe legal practitioners. Increasingly the courts, litigants, prosecutors, participants in the legal system, business and commerce and all other end-users are having to grasp at least some of the intricacies and complexities of information and communication

8 Section 1 of the ECT Act defines it as an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer.

9 *In re DoubleClick* (See website address in bibliography).

10 According to Van der Merwe (2008: 12), convergence can be defined as the merging of telephone, broadcasting and computing technologies, industries and cultures.

11 Some recent examples include the Labour Court decisions in *Jafta v Ezemvelo KZN Wildlife* where a valid employment contract was concluded via SMS, *Mafika v SA Broadcasting Corporation Ltd* where a valid resignation was affected via SMS, and the Supreme Court of Appeal decision on electronically stored wills in *Van der Merwe v The Master of the High Court and Another*, where an electronic version of a will was condoned under Section 2(3) of the Wills Act 7 of 1953 (for a commentary on this case see Papadopoulos – *SA Mercantile Law Journal* 2012, Vol. 1).

technology law.[11] The aim of this book is therefore to provide specialist insight into the myriad legal issues generated by the convergence of technologies and the rise of the internet, starting with a short synopsis of the legislation that forms the backbone of digital jurisprudence.

1.2 THE GROWING BODY OF SOUTH AFRICAN LEGISLATION

1.2.1 The Constitution

It is common knowledge that the Constitution of the Republic of South Africa, 1996, informs all other legislation or law which has to conform to the entrenched constitutional norms or face being struck down as unconstitutional.

The main constitutionally protected provisions which are of particular relevance in this subject area are contained in Section 14, the right to privacy, Section 16, the right to freedom of expression, and Section 32, the right of access to information (given effect in the Promotion of Access to Information Act 2 of 2000), all of which are discussed in further detail in later chapters of this book.

1.2.2 The Promotion of Access to Information Act 2 of 2000 (PAIA)

This legislation exists to give effect to the constitutionally guaranteed right of access to information,[12] and it allows access to both hard copy (*written*) and electronic records that contain personal information.[13]

To access information or records in either the public or private sectors certain conditions need to be met, such as:[14]

- The information/record is required for the requester to exercise or protect rights (Section 9(a).
- All proper procedures are complied with (Section 11(1)(a).
- The information requested should not fall within the categories of mandatory or discretionary grounds for refusal (Section 11(1)(b) and Sections 33–46).[15]

It is further an offence to destroy, damage, alter, conceal or falsify a record with the intention to deny a requester's access to the record (Section 90).

The Act does however protect against unreasonable privacy infringements, and provides some transparency on what and how information should be kept (Sections 34–63).

1.2.3 The Electronic Communications and Transactions Act 25 of 2002 (ECT Act)

This Act is comprehensively discussed throughout this publication and forms one of the cornerstones of information and communications technology law or cyberlaw. It is perhaps unique in the world in that it covers such a wide variety of topics in one omnibus act.

Notably in Chapter II of the ECT Act a national e-strategy is detailed which must among others devise strategies and programmes to provide internet connectivity to disadvantaged communities that include making facilities and infrastructure available or accessible. Unfortunately this has not been put into proper effect, and is an area that has been and still is beset with hurdles.[16] This issue is taken up in Chapter 3 which focuses on the regulation of the telecommunications sector.

12 In terms of Section 32 of the Constitution – see the preamble to PAIA.

13 Sections 3–8 of PAIA. Under Section 1 a "record" is information: (a) regardless of form or medium; (b) in the possession or under the control of that public or private body, respectively; and (c) whether or not it was created by that public or private body, respectively. This would include information recorded in any electronic or hard copy form or medium, including memos, letters, notes, e-mails, audio or visual or video recordings, computer data, etc.

14 Section 3 of PAIA.

15 Section 11(1)(b) and Sections 33–46. For example, access to information is prohibited if it would lead to an unreasonable infringement of a third party's privacy, i.e. in terms of Sections 34 and 63.

16 To such an extent that an entire chapter entitled "Telecommunications legislation and barriers to e-commerce" was included in Buys & Cronjé (2004:250–276). See also litigation such as *Altech Autopage Cellular (Pty) Ltd v Chairperson, Council of the Independent Communications Authority of South Africa*.

1.2.4 The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)

This is legislation that is primarily aimed at the interception and monitoring of communications and the provision of communication-related information within South Africa.[17]

Section 2 of RICA prohibits the interception[18] of a communication, in the course of its occurrence or transmission, which takes place outside the parameters of the Act. There are, however, certain statutory exemptions (where an interception direction is not necessary), such as:

- When the intercepting party is also a party to the intercepted communication (Section 4).
- When a party to the communication has given prior written consent to the interception (Section 5).
- When the interception occurs in connection with the carrying on of a business, and then only an indirect communication may be intercepted (Section 6).[19]
- Where the interception is to prevent serious bodily harm (Section 7).
- To locate a person in the case of an emergency (Section 8).
- When interception takes place in a prison (Section 9).
- When the monitoring of a signal takes place for maintenance or installation purposes or for managing the radio-frequency spectrum (Sections 10–11).

Chapter 3 details the process and requirements that need to be followed in order to obtain an interception order, decryption direction or entry warrant. These can only be issued by a judge at the request of an applicant law enforcement official who will have to prove that there is a reasonable suspicion that a serious crime has been or is about to be committed (Sections 16–25).

In order to give effect to the Act, Section 30 requires a telecommunication service provider (TSP) to provide a telecommunication service which has the capability of being intercepted and to store communication-related information. In addition, TSPs also have to collect and collate detailed personal information from both natural persons and juristic entities before concluding contracts for the provision of telecommunication services (Section 39).

By far the most controversial section of the Act is Section 40, which stipulates that a TSP may not activate a SIM card or allow the use of a cellphone on its telecommunications system unless the particulars of the SIM card or cellphone are recorded. The information required includes:

- The mobile subscriber integrated service digital network number (MSISDN number) of the SIM card to be activated.
- The international mobile equipment identity number (IMEI number).

17 Communication-related information includes "any information related to an indirect communication which is available in the records of a telecommunications service provider and includes switching, dialing or signaling information that identifies the origin, destination, termination, duration and equipment used in respect of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and where applicable, the location of the user". Section 1 of RICA.

18 Interception is defined as an aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes: (a) the monitoring of any such communication by means of a monitoring device; (b) viewing, examination or inspection of the contents of any indirect communication; and (c) the diversion of any indirect communication from its intended destination to any other destination, and "interception" has a corresponding meaning. Section 1 of RICA.

19 In Section 1 of RICA, a distinction is drawn between direct and indirect communications. A direct communication is an oral communication, other than an indirect communication, between two or more persons in the immediate presence of all other persons participating in the communication; or it is an utterance by a person participating in an indirect communication if the utterance is audible to another person, who at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication. This would, for example, include a telephone conversation. An indirect communication, on the other hand, is the transfer of information, including a message or part thereof either in the form of speech, music, sound, data, text, visual imagery, signals, radio-frequency spectrum or in any other form or combination of forms, that is transmitted in whole or in part by means of a postal service or telecommunication system.

- The full names, identity number and residential address, business and postal address of the SIM card user.

This requirement meant that TSPs had to embark on an extensive, costly exercise to verify the details of millions of prepaid cellphone users or face severe fines.

1.2.5 The Electronic Communications Act 36 of 2005 (ECA) and the Independent Communications Authority of South Africa Act 13 of 2000 (ICASA)

The ECA was promulgated to promote convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors and to provide the legal framework for convergence of these sectors; to make new provision for the regulation of electronic communications services, electronic communications network services and broadcasting services; to provide for the granting of new licences and new social obligations; to provide for the control of the radio-frequency spectrum; to provide for the continued existence of the Universal Service Agency and the Universal Service Fund; and to provide for matters incidental thereto (Preamble to the ECA). This Act works hand-in-hand with the ICASA Act.

These enactments and their implications are discussed further in Chapter 3.

1.2.6 The Protection of Personal Information Bill B9 of 2009 (PPI)

Many technologies associated with the internet have a real impact on people's privacy. Part of these issues around privacy can be attributed to the fact that computers were built to collect, compile and store large volumes of information. The widespread use of digital cameras, cellphones, geo-identification technology and GPS, coupled with the internet, where there are improved search engine capabilities and an infinite number of ways to intercept, store, match, share, mine and collate information making data protection imperative.

Traditional delictual jurisprudence only provides limited protection for an individual's personal information because, it can only assist in determining when the collection and processing of data is lawful or not. It cannot ensure that the individual is aware that information is being collected (Roos in Van der Merwe 2008:358). It is therefore essential for the legislature to enact legislation to protect personal information and conform to international data protection imperatives.

With this in mind the Protection of Personal Information (PPI) Bill was published in 2009.[20] The PPI aims to promote the protection of personal information processed by public and private bodies; to introduce information protection principles and to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Protection Regulator; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making and to regulate the flow of personal information across the borders of the Republic of South Africa (Preamble to PPI).

This enactment and its implications are discussed further in Chapter 13.

1.3 CONCLUSION

The legislation discussed in the preceding paragraphs represents only the most significant enactments that directly relate to the growing body of law in this subject area. Many other enactments have been amended in order to keep abreast of the advances of technology[21] and it seems that we can look forward to more enactments and/or amendments in the future with announcements such as that of the South African Law Reform Commission (SALRC), who have released an issue paper on *Electronic evidence in criminal and civil proceedings: admissibility and related issues* (Issue paper 27, project 126, 2010. See website address in bibliography).

In view of the impact of technology and the growing information revolution, as you read through the chapters that follow, the author trusts that you will be able to posit the principals of digital jurisprudence implemented through the interpretation of the law, common law and future legislative developments, international best practice, technological regulation and contract, and that this dynamic and complex area of the law will become more explicable.

20 Protection of Personal Information Bill, B9–2009 published in *Government Gazette* No. 32495 of 14 August 2009.

21 See, for example, the Copyright Amendment Act 125 of 1992 which created a new category of copyrightable works, namely computer programs.

BIBLIOGRAPHY

Books and reports

Buys, R. & Cronjé, F. (Eds). 2000. *Cyberlaw@SA: the law of the internet in South Africa*. 1st ed. Pretoria: Van Schaik.
Buys, R. & Cronjé, F. (Eds). 2004. *Cyberlaw@SA II: the law of the internet in South Africa*. 2nd ed. Pretoria: Van Schaik.
Fitzgerald, B., Fitzgerald, A., Middleton, G., Lim, Y. & Beale, T. 2007. *Internet and e-commerce law: technology, law and policy*. Sydney: Lawbook Co.
Hofman, J., Johnston, D., Handa, S. & Morgan, C. 1999. *Cyberlaw: a guide for South African doing business online*. Cape Town: Ampersand.
Lessig, L. 2002. *The future of ideas: the fate of the commons in a connected world*. New York: Random House.
Rooney, D., Hearn, G.E. & Ninan, A. (Eds). 2005. *Handbook on the knowledge economy*. Cheltenham: Edward Elgar.
Van der Merwe, D.P. 2000. *Computers and the law*. Cape Town: Juta.
Van der Merwe, D.P. 2008. *Information and communications technology law*. Durban: LexisNexis.

Journal articles

Papadopoulos, S. 2012. Electronic wills with an aura of authenticity. *SA Mercantile Law Journal*, 24(1).

South African cases

Altech Autopage Cellular (Pty) Ltd v Chairperson, Council of the Independent Communications Authority of South Africa, Case No. 20002/08, North Gauteng High Court
Jafta v Ezemvelo KZN Wildlife 2008 10 BLLR 954 (LC)
Mafika v SA Broadcasting Corporation Ltd 2010 5 BLLR 542 (LC)
Van der Merwe v The Master of the High Court and Another (605/09) 2010 ZASCA 99 (6 September 2010)

International cases

American Civil Liberties Union v Reno 929 F Supp 824 at 830–845 (ED Pa 1996)
In re DoubleClick Privacy Litigation 154 F Supp 2d 497 at 501–2 (SDNY 2001)
Dow Jones & Company, Inc. v Gutnick 2002 210 CLR 575; 2002 HCA 56 at 16

Legislation

Constitution of the Republic of South Africa, 1996
Copyright Amendment Act 125 of 1992
Electronic Communications Act 36 of 2005
Electronic Communications and Transactions Act 25 of 2002
Independent Communications Authority of South Africa Act 13 of 2000
Promotion of Access to Information Act 2 of 2000
Protection of Personal Information Bill, B9-2009
Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Web resources

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. & Wolf, S. [s.a.]. Brief history of the internet. Available at http://*www.isoc.org/internet/history/brief.shtml*

Republic of South Africa (RSA). 2009. Protection of Personal Information Bill. B9-2009. Available at *http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf*

South African Law Reform Commission. 2010. Issue Paper 27 Project 126. Electronic evidence in criminal and civil proceedings: admissibility and related issues. Available at *http://www.justice.gov.za/salrc/ipapers/ip27_pr126_2010.pdf*

US Department of Commerce. 2000. *Digital economy 2000*. Available at *http://www.esa.doc.gov/sites/default/files/reports/documents/digital_0.pdf*

US States District Court for the Southern District of New York. 2001. *In re DoubleClick, Inc. Privacy Litigation* 154 F Supp 2d 497 at 501-2 (SDNY 2001). Available at *http://cyber.law.harvard.edu/is02/readings/doubleclick.html*