

TECHNOLOGY

MEDIA AND TELECOMMUNICATIONS

ALERT

28 November 2012

CHANGING THE ELECTRONIC COMMUNICATIONS LANDSCAPE

The electronic communications sector and the use of electronic transactions have seen rapid growth in the last few years.

As a result of the population's ever increasing dependence on the internet there has been a significant rise in hacking, security breaches, misuse of personal information, cyber security threats and cyber-crime. As a result of these trends and in an attempt to ensure that South Africa measures up to international best practice, the Minister of Communications, on 26 October 2012, published the Electronic Communications and Transactions Amendment Bill (Bill) inviting the public to submit written comments to the proposed amendments to the Electronic Communications and Transactions Act, No 25 of 2002 (Act).

The Bill seeks to align our legislation with international standards and trends. A notable effort has also been made to align the Bill with the provisions of recent developments in our law, specifically the promulgation of the Consumer Protection Act, No 68 of 2008 and anticipated data protection legislation.

This article focuses on the more noteworthy amendments proposed under the Bill.

New definitions

Several new definitions have been included in the Bill. The definition of 'electronic transactions' has been expanded to include both commercial and non-commercial transactions. This feeds into the new definition of 'unsolicited communications'. A communication regarding any electronic transaction will be regarded as unsolicited unless the communication has been requested by the recipient.

The definition of 'service provider' presently incorporates only internet service providers. The Bill proposes extending the definition to include wireless application service providers who in addition to being expressly subjected to the provision of the Act will also, to the extent that they act as mere conduits for communications, benefit from the limitation of liability contained in the Act. The implications of this are examined in greater detail

IN THIS ISSUE

- **Changing the electronic communications landscape**
- **Electronic communications and transactions buzz**

in our article entitled Electronic Communications and Transactions buzz that is published below.

The definition of 'cryptography provider' has been streamlined to clarify the legislature's requirement that only people who are entities that develop cryptography products and services will be regarded as a 'cryptography providers'. The ambiguity that allowed for end users and installers of encryption software to be regarded as cryptography providers will be removed.

Spam

A specific object of the Bill is to minimise or eradicate spam. For this reason the new definition of unsolicited communications has been incorporated. Notably internet and wireless application service providers who send data messages to persons who have not implicitly or expressly requested the messages could face tough criminal sanctions in future.

Compliance with data protection principles

In terms of the Act as it stands, a data controller - any person who electronically requests, collects, collates, processes or stores personal information - may voluntarily comply with the principles governing the processes of electronically collected personal information. The Bill suggests that in future all data controllers be required to subscribe to the principles and record the fact that they have done so in an agreement with the data subject.

e-Strategy development

The draft legislation seeks to task the Minister with the responsibility of developing the national e-strategy and proposes that the Minister take account of international best practice and the laws and

continued

guidelines of other jurisdictions and international bodies, as well as existing laws within the Republic. The national e-strategy will focus on e-readiness, SMME development, human resource development and education and training in the ICT sector. This will greatly assist in enabling use of the internet and bridging the current digital divide.

e-Evidence and contracts

The provisions pertaining to the admissibility of online communications as evidence in a court and what constitutes a contract is broadly in line with the rules developed by United Nations Commission on International Trade Law and the position broadly adopted by the international community. In determining the evidentiary weight of a data message the Bill requires that regard must be had to the manner in which its originator was identified. The Bill proposes that the Act be expanded to include identification by way of an electronic signature.

Cryptography providers

The Bill proposes the introduction of specific objectives in relation to cryptography providers and their services and products. The Bill provides that cryptography providers should ensure conformance with all decryption directions under the Regulation of Interception of Communications and Provision of Communication-related Information Act, or any other laws of the Republic, as well as renew their cryptography provider-registration every two years.

Accreditation Authority

The Bill introduces the establishment of an Accreditation Authority to accredit certain types of electronic transaction service providers. The Accreditation Authority will also monitor compliance with the Act.

The Bill proposes the introduction of mandatory registration of authentication service providers, products and services.

At present only South African accredited 'certification service provider' can issue advanced electronic signatures. The Bill provides that electronic signatures accredited in a foreign jurisdiction be recognised in South Africa provided there is a recognition agreement in place.

Deemed recognition of representative bodies

The Act currently excludes liability on the part of a service provider to act as mere conduits of information. In order for a service provider (which, if the Bill is passed, would include wireless application service providers) to benefit from the limitation of liability provisions in the Act they are required to belong to an industry representative body recognised by the Minister and must subscribe to the code of conduct of that representative body.

In order to facilitate the recognition of industry representative bodies, the Bill suggests that representative bodies be deemed recognised if, after a period of 12 months after application has been made for recognition, the Minister has not responded to the application.

Cyber security hub

The Bill proposes that the Minister establish a cyber security hub for creating, amongst other things awareness of threats to electronic communications networks and communications from cyber-crime.

The aim of the hub would be to respond to cyber security incidents, creating guidelines to educate persons about cyber-crime, centralising coordination of cyber security activities, conducting cyber security audits, and fostering and promoting cooperation between government and interest groups in implementing cyber security standards.

Penalties

A number of hefty penalties for contravention of the Act are proposed in the Bill:

- A person who transmits unsolicited communications may be liable of a fine up to R1 million or a period of imprisonment not exceeding one year.
- A person providing cryptography products or services without registering with the Department of Communications or failing to provide information may be subject to a fine up to a maximum of R2 million.
- A person falsely holding out their products or services have been accredited may be subject to a fine of not more than R2 million or a prison term of not more than two years.
- A person who discloses information which is declared by the Minister to be of importance to the protection of national security or the economic and social well-being of its citizens such as 'critical information' may be fined up to R5 million or imprisonment of three years.
- A person who, without authorisation, accesses or intercepts data is liable to conviction of a fine not exceeding R10 million or imprisonment of ten years – this includes a person who after becoming aware of the fact that he or she is not authorised to access the data continues to access or use that data.

The Bill is a significant piece of legislation and will affect, in particular, the businesses of internet service providers and wireless application service providers. In our view the drafters of the Bill should be commended for incorporating many of the amendments proposed by the South African Law Reform Commission in 2011 as well as attempting to harmonise the Act with other South African legislation and international best practice.

Written representations are due on or before 7 December 2012. This deadline may be changed if the Department of Communications is amenable to the representations made by various industry organisations to the effect that the deadline be extended until January 2013.

Kathleen Rice, Mariska van Zweel and Anushka Bhawan

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BUZZ

The Electronic Communications and Transactions Amendment Bill, 2012 (Bill) is likely to cause a buzz among wireless application service providers (WASPs).

The Bill proposes extending the application of the consumer protection provisions of the Electronic Communications and Transactions Act, 2002 Act) to wireless application services with the aim of minimising the transmission of spam or preventing it altogether. In addition, the seven day cooling off period contained in the consumer protection chapter of the Act will apply to WASPs. It is not all doom and gloom for the WASP industry as the limitations of liability provisions of the Act will be extended (eventually) to apply to certain WASPs if the Bill is passed in its current form.

Unsolicited communications

Presently, in terms of the Act, a person sending unsolicited commercial communications must provide the consumer with an option to cancel a subscription and must provide the consumer with identifying particulars from which the sender of the communications obtained the consumer's personal information if so requested by the consumer.

A definition for 'unsolicited communications' has been suggested in the Bill. In terms of the Bill, a communication message regarding goods or services transmitted to a consumer by or behalf of the supplier without the consumer having expressly or implicitly requested that message, constitutes 'unsolicited communications'. The Bill, if passed in its current form, will make the transmission of unsolicited communications unlawful. The definition of 'unsolicited communications' is wider than the definition of 'spam' contained in the Wireless Application Service Provider Association (WASPA) Code of Conduct (Code). The Code excludes messages sent to consumers with whom there is a prior commercial relationship from the definition of 'spam'. The Bill does not give this latitude.

The Consumer Protection Act, No 68 of 2008, (CPA) also deals with unsolicited communications. In terms of the CPA a person may refuse to accept so-called 'direct marketing' (that would include messages for goods and services sent by WASPs) by demanding that the person responsible for initiating the communication desist from any further communication or by registering a pre-emptive block with a person managing a registry recognised by the National Consumer Commission (Commission). A direct marketer must, in terms of the CPA regulations, assume that a potential recipient of a message has registered a pre-emptive block unless the direct marketer has proof that the recipient has expressly consented to receiving direct marketing from the direct marketer. It is therefore incumbent upon the direct marketer to interrogate the registry prior to sending direct marketing messages. These provisions of the CPA are of little or no effect until such time the Commission recognises a registry.

The Bill goes a step further than the CPA. While the CPA allows for consent to receive messages, the definition of 'unsolicited

communications' requires that the recipient 'request' the message. The proposed wording of s42(1) states that no person may send unsolicited communications without the 'permission' of the consumer to whom the unsolicited communications are being sent. The proposed amendment requires some refinement given that the definition of 'unsolicited communications' incorporates reference to a consumer request which is more onerous than the requirement for permission.

What will cause some alarm is that the Bill makes provision for the imposition of a fine up to a maximum of R1 million or imprisonment for a period not exceeding one year if a person sends unsolicited communications. The criminal sanction would presumably be over and above any sanction imposed by an industry association such as WASPA.

Cooling off period

The Bill proposes the extension of the definition of 'service provider' to incorporate persons providing wireless application services. The category of 'persons providing wireless application services' is a wider category of service providers than WASPs as defined in the Bill as the definition in the Bill defines a WASP as a person who has concluded an agreement with an electronic communications licensee enabling the provision of wireless application services. Not all persons providing wireless application services have concluded agreements directly with electronic communications licensees.

An implication of the extension of the definition of 'service provider' is that the cooling off period contained in s44 of the Act will become applicable to persons providing wireless application services regardless of whether those persons have concluded agreements directly with electronic communications licensees. Accordingly, a consumer may cancel without reason and without penalty, any transaction for the supply of services or goods within seven days after the date of conclusion of the agreement. If the consumer does so, he/she will be entitled to a full refund within thirty days of cancellation. From the perspective of a person providing wireless application services there is a potential that consumers will receive and consume services for a period of seven days and then terminate the agreement demand repayment of subscription fees.

Protection of personal information

The Act contains a number of principles set out in s51 for electronically collecting personal information. These principles are aimed at protecting private personal information and include an obligation to obtain express permission for the collection and processing of personal information, disclosure in writing of the specific purpose for which personal information is requested, record-keeping, nondisclosure obligations and requirements to destroy obsolete personal information.

Presently, data controllers (ie any person who electronically requests, collects, collates, processes or stores personal information) may voluntarily subscribe to the principles. The Bill requires that each data controller subscribe to the principles and must, in addition record the fact that it has subscribed to the principles in any agreement with a data subject.

Limitation of liability

The Act exempts 'service providers' from liability to the extent that the service provider concerned acts as a mere conduit for information in that it does not initiate the transmission, does not select the addressee, or perform its functions in an automatic, technical matter without selection of data and does not modify the data contained in the transmission.

Presently the limitation of liability only applies to Internet service providers. A consequence of extending the definition of 'service provider' is that the benefits of the exclusion of liability provisions of the Act will be extended to WASPs. WASPs who provide content and who select the addressees will not however benefit from the amendment if it is affected.

In addition, the Bill provides that, in order to benefit from the limitation of liability provisions, the service provider that acts as a mere conduit must be a member of a representative body recognised by the Minister of Communications and the service provider must have adopted and implemented the code of conduct. WASPA would

need to be recognised by the Minister as a representative body before any WASP can take advantage of the limitation of liability provisions contained in the Act. The Bill proposes that a representative body that applies to the Minister for recognition will be deemed to be recognised after a period of twelve months has elapsed from the date of application if the Minister has not indicated to the contrary. While the deeming provisions may be welcomed by representative bodies, for many the period of 12 months may seem inordinately long and a positive obligation on the Minister to act within a reasonable period of time would be preferred.

The proposed amendments to the Act are wide ranging and the effects of certain amendments on WASPs are but one aspect that requires careful consideration. Written representations are due on 7 December 2012 and a number of industry associations have expressed reservations regarding the feasibility of this deadline. In our view, given the ramifications of the amendments and the range of interested parties affected thereby, it would be appropriate for the Department of Communications to extend the deadline.

Kathleen Rice

CONTACT US

For more information about our Technology, Media and Telecommunications practice and services, please contact:



Preeta Bhagattjee
Director
National Practice Head
T +27 (0)11 562 1038
E preeta.bhagattjee@dclacdh.com



Ridwaan Boda
Director
T +27 (0)11 562 1037
E ridwaan.boda@dclacdh.com

Leishen Pillay
Senior Associate
T +27 (0)11 562 1265
E leishen.pillay@dclacdh.com



Clem Daniel
Director
T +27 (0)11 562 1073
E clem.daniel@dclacdh.com

Tayyibah Suliman
Senior Associate
T +27 (0)11 562 1248
E tayyibah.suliman@dclacdh.com



Simone Gill
Director
T +27 (0)11 562 1249
E simone.gill@dclacdh.com

Mariska van Zweel
Associate
T +27 (0)11 562 1180
E mariska.vanzweel@dclacdh.com



Kathleen Rice
Director
T +27 (0)11 562 1036
E kathleen.rice@dclacdh.com

Victor Omoighe
Associate
T +27 (0)11 562 1209
E victor.omoighe@dclacdh.com

This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

BBBEE STATUS: LEVEL THREE CONTRIBUTOR

www.cliffedekkerhofmeyr.com

©2012

Cliffe Dekker Hofmeyr is a member of DLA Piper Group,
an alliance of legal practices