Comments on the Cybercrimes and Cybersecurity Bill [B6 – 2017]

Prepared by Jacques Allers

TABLE OF CONTENTS

SCOPE

The Cybercrimes and Cybersecurity Bill was published on 28 August 2015. This bill aims to protect against criminal, terrorist and other illicit cyber activity and consolidates South Africa's cybercrime laws into one place. It affects all companies and individuals concerned with IT (and POPI) regulatory compliance; all Electronic Communications Service Providers (ECSPs); representatives from various government Departments; so-called cyber criminals and terrorists; developers and providers of software or hardware tools that could be used to commit offences; financial services providers because there are some prohibited financial transactions; information security experts; all owners of "information infrastructure" that could be deemed critical by Government; and finally all internet and computer users. Copyright and intellectual property owners are no longer directly dealt with but i.t.o. clause 11(2), offences of interfering with data, a computer program, computer data storage medium or a computer system and cyber extortion which causes the destruction of or substantial damage to any property are regarded as aggravated offences which are punishable with a sentence, as provided for in section 276 of the Criminal Procedure Act, 1977.

PENALTIES

This bill creates roughly 50 new offences (specifically relating to data, messages, computers and networks). Specifically, the use of personal or financial information to commit an offence; hacking; the unlawful interception of data; all forms of computer related forgery and uttering; and any form of computer-assisted extortion or terrorist activity. The penalties range from one year to ten years imprisonment or R1 million to R10 million (i.e. R1 million for each year of imprisonment). The most common penalties, are either R5 million or five years, or R10 million or ten years imprisonment.

POLICE, STATE SECURITY AND THE ESTABLISHMENT OF SECURITY CENTRES

Provided a valid search warrant, the Bill gives the South African Police Service and the State Security Agency (and their members and investigators) extensive powers to

investigate, search, access and seize any electronic/computing device (i.e. a computer, database server or entire network). Foreign states and South Africa will co-operate to investigate cybercrimes and the Minister of Police must establish and operate (through the appointment of a Director) a 24/7 *Point of Contact center* for cyber crimes. A National Cybercrime Centre (with another appointed Director) must also be established.

Furthermore, the Bill creates a Cyber Response Committee made up of about 13 people. The chairperson will be the Director-General: State Security. The Minister of State Security must establish and operate a Cyber Security Centre and appoint an individual from the State Security Agency as its Director, and one or more Government Security Incident Response Teams (with a person from the State Security Agency being appointed as the head of each one).

A Cybersecurity Hub must also be established and operated by the Minister of Telecommunications and Postal Services (with a Director being appointed to it) and Electronic Communications Service Providers will be required to operate (at their cost) Private Sector Security Incident Response Teams.

The Bill furthermore aims to identify, declare and protect National Critical Information Infrastructure, like the Department of Home Affairs database. The Bill also creates a National Critical Information Infrastructure Fund for the management of disasters. There are various obligations on the owner of (or person in control of) a National Critical Information Infrastructure.

The Bill also aims to empower the general public to admit evidence of cybercrimes.

THE EXPECTED ROLE OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS (ESCP)

The Cybercrimes and Cybersecurity Bill defines Electronic Communications Service Providers very broadly. An ESCP includes a person who provides an electronic communications service with an electronic communications service licence; a financial institution for example a bank; or anyone (including an entity) who processes or stores data for someone else – an ESCP is thus essentially "everyone".

The Bill places some onerous legal obligations on ECSPs, including the reporting of cybercrimes to the police (via the National Cybercrime Centre) and the storing evidence about cybercrimes. Non-compliant parties will be fined R10 000 per day. Specifically, i.t.o. clause 52(1), an electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of offences provided for in Chapter 2 and which is determined in terms of subclause (2), must without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and preserve any information which may be of assistance to the law enforcement.

READ WITH POPI

South Africa's Protection of Personal Information Act seeks to regulate the Processing of Personal Information and thus directly impacts the daily operations of companies in terms

of how personal information is used and processed. Noncompliance with the provisions set out in the Act can result in significant fines and criminal sanctions being levied against companies, directors and employees.

Clause 2 of the Cybercrimes and Cybersecurity Bill states that any person who unlawfully and intentionally secures access to data is guilty of an offence and on conviction can be liable for a fine of up to R5 million or imprisonment of up to 5 years. On the face of it, it is prudent to state that no one should unlawfully access data, but the consequences of such a widely drafted provision can be far-reaching. The term "access", amongst others, includes: to make use of, view, store, copy or remove data. "Unlawful" includes any action where a person exceeds his lawful authority to access data. Read with the POPI Act (and once POPI is fully operational) this clause of the Bill will criminalise any access to data which goes beyond a person or entity's authority. In other words, if a person or company does not have an individual's consent to use or store his/her data in a certain manner or for a certain purpose, as contemplated in POPI, that person or company will be accessing his data unlawfully, as contemplated in clause 2 of the Bill.

Similar provisions apply to any person who manufactures, sells, advertise, uses or possesses software that can be used for the purpose of contravening the provisions of clause 4. Thus, the developers and users of software that operates like cookies or other similar technologies used for advertising, research and analytics, will have to ensure that the software does not collect data beyond what it is authorised to do, or face a fine of up to R5 million or imprisonment of up to 5 years.

The Bill thus imposes potentially onerous obligations on electronic communications service providers, which are defined so wide that it will include any person or entity which transmits, receives, processes or stores data on behalf of any other person.

PREVIOUS ISSUES

The Bill is no longer as excessively far-reaching as the initial draft, and it limits the level of discretion granted to the State's security cluster. The clauses that do address cybercrime is also much more specific. For instance, clause 7 used to address the unlawful acquisition of personal and financial information with the intention of committing an offence (and it was linked to the POPI Act). This clause has now been narrowed to deal with the unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices. Similarly, clause 9 now deals with unlawful acts in respect of cyber forgery while clause 10 addresses the unlawful and intentional offence of cyber extortion. Copyright infringement is no longer dealt with under clause 20 (or directly anywhere else in the Bill). That said, Clause 3 creates the offence of **unlawful acquiring of data**. The offence aims to protect data which is stored or transmitted over an electronic communications system. The offence criminalises the overcoming of protection measures which are intended to prevent access to data and thereafter to acquire data within, or which is transmitted to or from, a computer system. The clause further criminalises the possession of data, with the knowledge that such data was acquired unlawfully; and the possession of data, in respect of which there is a reasonable suspicion that such data was acquired unlawfully where the possessor is unable to give a satisfactory exculpatory account of such possession. ''Data'' is, however, defined as electronic representations of information in any form – it's thus not too far a stretch to assume that copyrighted content in digital form qualifies.

In the initial analysis of the 2015 Bill, it seemed that the South African Police Service and the State Security Agency were granted overly far-reaching powers to investigate, search, access and seize literally any electronic device, with verbally granted search warrants being deemed sufficient to take action as deemed appropriate. In the 2017 draft, clause 27 provides that an article may only be searched for, accessed or seized by virtue of a search warrant issued by a judicial officer if it appears to the judicial officer, from information on oath or by way of affirmation that there are reasonable grounds for believing that an article is being used or is involved in the commission of an offence or is required as evidence at criminal proceedings.

ESCPs will be subject to clause 52 of the Bill – specifically, ESCPs will be required to keep their customers updated about cybercrime trends but no guidance as to the frequency of these updates are given (nor the mode of communication that should be employed). Would a company or juristic body be non-compliant if a customer exercised his/her rights to privacy as described in the POPI Act (by expressly stating that he/she does not want to receive communication from said company)? This clause also requires that companies preserve any information that may be of assistance to the law enforcement agencies investigating an offence, including origin, destination, route, time, date, size, duration and type of services. If a ESCP's infrastructure is not able to track (or store) those – or if the offender is using encryption, would the ESCP still be held liable?

It's important to note that comments on the Bill should reach the Department by 28 July 2017.

CONCLUSION

The amended Cybercrime and Cybersecurity Bill aims to create cybercrime offences as well as penalties. The proposed offences deal with the protection of confidentiality, integrity and the availability of computer data and include unlawful access, the interception of and/or interference with protected data, the deployment of malware, password-infringements, etc.

The Bill thus criminalises cyber-offences in terms of fraud, forgery, uttering and extortion. Specifically, in terms of the Bill the following are identified as criminal activities:

- unlawful securing of access to data, a computer program, a computer data storage medium or a computer system;
- unlawful acquisition of data;
- unlawful acts in respect of software or hardware tools;
- unlawful interference with data or a computer program;
- unlawful interference with a computer data storage medium or computer system;
- unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices;
- cyber fraud;
- cyber forgery and uttering;
- cyber extortion;
- certain aggravated offences;
- attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence;
- theft of incorporeal properties;

- unlawful broadcast or distribution of data messages which incites damage to property or violence;
- unlawful broadcast or distribution of data messages which is harmful; and
- unlawful broadcast or distribution of data messages of intimate image without consent.

Furthermore, the penalties imposed by the Bill range from fines to imprisonment for up to 15 years.

The Bill is in-line with international best practice as it criminalises not only unlawful and intentional cybercrime but creates new crimes for cyber fraud, cyber forgery and cyber uttering. It also criminalises malicious communication – i.e. online communication that may result in harm to a person's property or personality.

The Bill also extends local jurisdiction for crimes not committed in South Africa but where the effect of those crimes are locally felt and a framework is created for the cooperation between foreign states regarding the investigation and prosecution of cybercrimes. To this effect, the South Africa Police Service is also given extended investigation, search and seizure powers. Obligations are also imposed on electronic communications service providers (for example, ISPs) and financial institutions to assist the SAPS in the investigation and reporting of cybercrimes,

For the first time, standard-operating procedures regarding cybercrime investigations are also being stipulated and a number of governmental and ministerial structures are created to detect and investigate instances of cybercrime – for example, a Cyber Response Committee tasked with the implementation of policies and a Cyber Security Hub to process information related to cybercrime.