PRESENTATION BY THE SOUTH AFRICAN POLICE SERVICE AND THE DIRECTORATE FOR PRIORITY CRIME INVESTIGATION TO THE SELECT COMMITTEE ON SECURITY AND JUSTICE NATIONAL COUNCIL OF PROVINCES

CYBERCRIMES BILL [B 6B-2017]

5 FEBRUARY 2020

Introduction

On assessment of the Cybercrimes Bill [B 6B-2017], the following clauses have an impact and refer directly to:

- The South African Police Service (SAPS)
- Minister of Police
- The National Commissioner of the South African Police Service (SAPS)
- The National Head of the Directorate for Priority Crime Investigation (DPCI)

Clause 1: Definitions and interpretation

(definitions of the National Commissioner, the National Head of the Directorate, police official and specifically designated police official)

Clause 20: Order to protect complainant pending finalisation of criminal proceedings

(laying of a complaint with the SAPS in respect of offences in clauses 14, 15 and 16)

Clause 24 (6): Jurisdiction

(directives regarding investigation of offences committed outside the RSA)

Clause 26(1): Standing Operating Procedures

(SOP's for the investigation of cybercrimes)

Introduction:

Clause 28: Search for, access to, or seizure of certain articles
(search and seizure by the SAPS)

Clause 29: Article to be searched for, accessed or seized under search warrant
(search and seizure by police official)

Clause 30: Oral application for search warrant or amendment of warrant
(oral application for search warrant by specifically designated police official)

Clause 31: Search for, access to, or seizure of article without search warrant with consent of person who has lawful authority to consent
(search and seizure by police official with consent)

Clause 32: Search for, access to, or seizure of article involved in the commission of an offence without search warrant
(search and seizure by police official without a warrant)

Introduction:

Clause 33: Search for, access to and seizure of article on arrest of person

(search and seizure by police official during arrest)

Clause 34: Assisting police official or investigator

(assistance to police official during search and seizure by person suspected to be involved or who is in control of system that is subject to investigation)

Clause 35: Obstructing or hindering police official or investigator and authority to overcome resistance

(Obstructing a police official)

Clause 36: Powers conferred upon police official or investigator to be conducted in decent and orderly manner with due regard to rights of other persons

(powers of police official subject to decency and order)

Clause 37: Wrongful search, access or seizure, and restriction on use of instrument, device, password or decryption key or information to gain access

(wrongful search and seizure and access by police official)

Introduction:

Clause 39: Prohibition on disclosure of information

(prohibition on disclosure of information by any person, including police official)

Clause 41: Expedited preservation of data direction

(expedited preservation of data direction by specifically designated police official)

Clause 42: Preservation of evidence direction

(application for preservation of evidence direction by police official)

Clause 43: Oral application for preservation of evidence direction

(oral application for preservation of evidence direction by police official)

Clause 44: Disclosure of data direction and search for, access to and seizure of article subject to preservation of evidence direction

(application for disclosure of data direction by police official)

Clause 45: Obtaining and using publicly available data or receiving data from person who has authority to disclose data

(obtaining and use of data by police official)

Introduction:

Clause 47: Spontaneous information

(National Commissioner or National Head may release information of investigations to a foreign State)

Clause 48: Foreign requests for assistance and cooperation

(foreign requests for assistance to be directed to the Point of Contact and powers of specifically designated police official)

Clause 52: Establishment and functions of designated Point of Contact

(establishment of the Point of Contact in the SAPS structures)

Clause 54: Obligations of electronic communications service providers and financial institutions

(obligations of electronic communication service providers/ financial institutions to report certain cybercrimes to the SAPS within 72 hours after becoming aware of such offences)

Introduction:

Clause 55: Capacity to detect, prevent and investigate cybercrimes

(Minister of Police **must** build capacity in the SAPS and report statistics)

Clause 59 (2): Regulations

(Minister of Police **must** make regulations in respect of clause 54 and **may** make regulations in respect of clauses 52 and 55)

Schedule to the Bill:

i.e. Section 71 of SAPS Act

Scope of the presentation:

Comments of the SAPS in this presentation is limited to inputs received that directly impact on/relate to the SAPS. Four proposals are made for (possible) amendment of the Bill. These proposals are highlighted in red in the submission.

Scope

SAPS received inputs from::

- 1. Anonymous
- 2. Centre for Applied Legal Studies: Faculty of Commerce, Law and Management: University of the Witwatersrand
- 3. Commission for Gender Equality
- 4. First Rand
- 5. JP Morgan
- 6. Media Monitoring Africa
- 7. MTN
- 8. TELKOM
- 9. VODACOM

- Only the submissions of entities listed from 4-9 are discussed since they made submissions which directly impact on/relate to the SAPS.

First Rand

Submission:

Clause 24 (6)- Clause provides for National Commissioner/National Head of Directorate, in consultation with the NDPP to **issue directives** which all SAPS officials are obliged to comply with in the execution of their functions in terms of the Act, insofar as it relates to investigating offences committed outside of the Republic.

Unclear what the **consequences** will be if a SAPS official fails to follow directives/ results in a monetary loss to a company and/or failing to secure a conviction.

Unclear what recourse a company would have - due to the negligence of SAPS official in failing to follow the directives.

Request **guidance to be provided**.

Reply:

Chapter 3: Clause 24: Jurisdiction

There will be consequences for SAPS officials - can be charged departmentally in terms of the SAPS Discipline Regulations.

Wrongful search, seizure and access by a police official is criminalised in terms of clause 37: “Wrongful search, access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access”.

It is also possible to address the consequences in the above-mentioned directives.

First Rand

Submission:

Chapter 4: Clause 26(1)- *issue Standard Operating Procedures (SOP's)* which must be observed by SAPS officials and any other person/agency authorised to assist with an investigation.

SOP's must be issued *within* ***6 months***- must follow a consultative process.

Principle of issuing SOP's supported- important that these procedures be clear/practical/effective- clear consequences for non-compliance be stipulated.

Rolled out with **adequate training**.

First Rand is of the view that the SOP's must be clear and practical, supported by rigorous training programmes.

Reply:

Chapter 4: Clause 26: Standard Operating Procedures

The capacity building obligations on the Minister of Police, in terms of clause 55 will address this aspect. In terms of this obligation the Minister of Police must establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes, ensure that members of the SAPS receive basic training in aspects relating to the detection, prevention and investigation of cybercrimes and in co-operation with my institution of higher learning, in the Republic or elsewhere, develop and implement accredited training programs for members of the SAPS primarily involved with the detection, prevention and investigation of cybercrimes.

Once in place, the SOP's will be rolled out by means of "workshops" and other training interventions.

First Rand

Submission:

Chapter 4 & broad definitions of ‘access’ and ‘seize’/references to right to access/seize throughout Chapter 4, most importantly s 28 and s 32 (without a search warrant).

Provides investigators with **far reaching powers to access (without limitation)**, as well as to seize.

No rights provided for a person to object to search and seizure.

Reply:

Clause 32: Search for, access to, or seizure of article involved in the commission of an offence without search warrant.

First Rand states that law enforcement has far-reaching powers without limitation and that there should be an opportunity for persons to object to search and seizure.

There are indeed limitations on police officials when they act without a warrant: see clause 32(2) *“…police official may only* ***access/perform powers in par c or d (copying/printout of data …. in accordance with a search warrant***” (NO WARRANT= LESS POWERS).

In the Criminal Procedure Act 51/1977 there is no provision made to object to a search, why should it be different in the online environment? Objections may unnecessary delay investigations and may be used by suspects in effort to evade justice.

Objections should be raised in a court of law or in litigation to nullify a warrant, not on a crime scene by a person (suspect) who does not want to be subjected to a search and seizure operation.

First Rand

Submission:

Chapter 4: Clause 28- Search for, access to or seizure of certain articles-**There are no rules regarding the execution of warrants.**

Rules exist under POPIA Clause 84.

There should be consistency as it relates to the rules for the execution of a warrant.

Reply:

Clause 28: Search for, access to, or seizure of certain articles.

There is no truth in this statement, rules have been laid down by court judgments, including the Constitutional Court.

SAPS/DPCI have National Instructions/National Directives/Circulars issued by the National Commissioner/National Head of the Directorate in respect of search and seizures and operations.

First Rand

Submission:

Clause 34- "**technical assistance and such other assistance as may be reasonably necessary**" to a SAPS official /investigator in order to search/access/seize an article.

Failure result in it being guilty of an offence and may be liable to a fine/2 years imprisonment/both.

Places an obligation on the financial institution to provide "technical" and "*such other assistance*" as required, **without taking into account** resources/capacity/ availability/normal day to day running of business.

"**such other assistance" as required is set out too broadly** and may even be something which the financial institution is unable to provide.

Proposed wording to be added:

*"… in terms of clause 29(1) should, if required, and insofar as it is **reasonable and practicably possible**, provide (a) technical assistance and (b) such other assistance…"*

First Rand is of the view that this provision should also provide for an **objection clause by a system owner.**

Reply:

SAPS is not in support since this may create a possible defence/excuse not to assist. The financial institution is in the best position to provide technical assistance during the search and seizure.

Objections can be raised in court/litigation.

These aspects can be addressed in the Standard Operating Procedures to be issued in terms of Clause 26.

First Rand

Submission:

Clause 43- Application in clause 42 to be made by way of *oral application* (as opposed to written application).

If granted, the outcome will be that a preservation of evidence direction will be issued

It is unclear what *maximum period applies in terms of preserving the evidence or if the **90-day** period, as referenced in clause 42, applies.*

Requested clarity be provided around what **maximum time period** applies, in terms of the preservation of evidence and/or if the 90-day time period, as referenced in clause 42, applies.

Reply:

Clause 43: Oral application for preservation of evidence direction.

Submission for specific time lines in clause 43 supported as it will enhance legal certainty.

First Rand

Submission:

Chapter 8: clause 54- Requires financial institutions, amongst others, to **report** to the SAPS within **72-hours** of becoming aware of a Cybercrime on their computer system and preserve any information which may be of assistance to law enforcement in investigating the offence.

Provision does not take into account that it **may not always be reasonable and/or practical** to report within that time period due to internal processes and/or business constraints.

No time period has been provided for preservation- cannot be held for indefinite period and a time frame must be applied.

Reasonable extension/ increased to 5 business days to afford the financial institution with adequate time to follow its internal processes and to ensure that it is reporting adequately and accurately.

First Rand wants the **72 hour** period to be extended to **5 business days.**

Reply:

The proposed period of 5 business days is too long in relation to the investigation and prevention of cybercrime and is not supported.

Rapid response is essential to preserve evidence.

Proposed that (only) reports in terms of clause 54 of the Bill be made to the SAPS Point of Contact –structure created by clause 52.

JP Morgan

Submission:

72hrs reporting timeframe seems reasonable.

JPMorgan Chase Bank Johannesburg Bank would **prefer no specific timeframe**, (we prefer the requirement to report be within a reasonable amount of time after confirmation that a breach/offence occurred).

The above comment would not require the firm to actively monitor its networks for evidence of a cybercrime and the 72 hour **clock starts ticking only after we are aware of the offence, not when we are aware of the activity.**

Reply:

Already addressed in response to First Rand.

Rapid response is essential to preserve evidence.

SAPS does not support the submission.

Media Monitoring Africa

Submission:

Inter alia expresses concerns that public officials involved in investigation and prosecution of cybercrimes are **(not) educated** in this regard.

Reply:

Capacity/Capability:

There is capacity in the SAPS.

Furthermore, clause 55 places an obligation on the Minister of Police to establish sufficient human and operational capacity to address cybercrime and to ensure that SAPS receives basic and specialised training.

MTN

Submission 1/3:

Chapter 4: Clause 25 - permits police official to access/seize the article which forms the subject of the investigation—MTN concerned **extensive seizure powers.**

Submit authority provided to in clause 29(1)(a) – Magistrate to authorise search and seizure warrant - be removed-replace with "**designated judge**' as defined in RICA.

MTN proposes that magistrate should not authorise a search warrant and that this authority must only be given to the designated judge of the RICA.

Submission 2/3:

Clauses 34 & 35- provisions be made –police official to be provided with a **digital copy** of the information required.

MTN proposes that the Standard Operating Procedures (SOP's) (Clause 26) take into consideration:

- That no action taken should impair the function of a computer or storage media.
- That no action taken should produce the effect of disrupting the service of an ECSP to its customers not implicated in the offence or reducing service quality to such persons.

MTN

Submission 3/3:

MTN submits that clause 25 allows the SAPS to seize the **actual electronic communications network** of a service provider and that limitations should be set to **only access control information**.

Clause 35: (Obstructing a police official)

MTN concerned that this clause/seizures by the SAPS may affect their daily operations and propose that the SAPS be provided with a digital copy of the information required.

MTN proposes an amendment to clause 59(2) to ensure that reports to the SAPS is made on a confidential basis.

MTN

Reply 1/3:

The submissions made by MTN may possibly be addressed during the public consultation process prescribed for the Standard Operating Procedures.

Clause 26(1): Standard Operating Procedures

(SOP's for the investigation of cybercrimes).

Clause 26 provides for public consultation on the SOP's.

In view of the extensive consultation process that will be required to address concerns of all these respondents it is proposed by the SAPS that the period of **6 months** within which the SOP's have to commence, be extended to **12 months**.

Definition of computer/computer storage medium too broad/vague, may lead to vague search warrants and directions:

- SAPS disagrees with this submission: Both of these concepts are defined extensively.
- MTN also did not make any proposal to address their concerns .

MTN

Reply 2/3:

Clause 29: Article to be searched for, accessed or seized under search warrant

(search and seizure by police official).

MTN proposes that Magistrate should not be authorised to issue a search warrant and that this authority must only be given to the designated judge of the RICA:

- This is impractical and will hamper the SAPS from doing their work.
- The CPA 51/1977 provides for Magistrates to issue warrants.
- Why is cybercrime treated differently?
- The RICA designated judge is responsible for applications in terms of RICA, not for applications in terms of the Cybercrimes Bill.

Clause 25: Definitions

MTN submits that clause 25 allows the SAPS to **seize** the **actual electronic communications network** of a service provider and that **limitations** should be set to only access control information.

It is further submitted that the Bill does not state clearly that businesses should be able to continue with their daily operations after a seizure.

No substantiation for this submission can be found in the definition of "seize". Limitations are set in accordance with the legislation and the judicial authority who approves the warrant. Police officials will also be guided by the SOP's that have to be drafted in terms of clause 26.

MTN

Reply 3/3:

Clause 35: Obstructing or hindering police official or investigator and authority to overcome resistance.

(Obstructing a police official)

MTN concerned that this clause/seizures by the SAPS may affect MTN daily operations and propose that the SAPS be provided with a digital copy of the information required.

As stated, this aspect can be provided for in the SOP's.

Clause 59: Regulations

(make regulations … category or class … form and manner …)

MTN proposes an amendment to clause 59(2) to ensure that clause 54 reports to the SAPS is made on a confidential basis.

This proposal is supported. (See also the proposal on slide 15.)

TELKOM

Submission:

Raise concerns with regard to powers to investigate, search, access and seize electronic communications (chapter 5), as well as obligations on electronic communications operators to preserve certain data.

f) When receiving **preservation orders** as envisaged in the Bill, ECSP might be placed in the situation that they **cannot comply in full or partially** with such orders because of *inter alia* **inadequate storage** capacity/hardware and software requirements- Telkom reiterates its concerns regarding the legal workload/costs to contest regular preservation orders on grounds of unreasonable expectations or substantive technical limitations- Telkom is concerned that **orders to preserve data** or evidence for the purposes of criminal proceedings in cases relating to cybercrime(s) may be served on an *ad hoc* basis, **impose a heavy burden** on operators depending on the nature of the information required and that the preservation of such information may in some instances be infeasible.

Emphasise that **clear SOP's** regarding the search and seizure of data, drafted in consultation with industry, is imperative to clarify the ambit of such directives as well as avoid any unintended effect on electronic communications networks as well as the interruption of electronic communications services to customers.

TELKOM

Submission:

Chapter 5 (Powers to investigate, search, access and seize)

Standard Operating Procedures

a) Emphasise the importance of **clear SOP's** to clarify the obligations set out in Chapter 5- support a process of consultation with industry when drafting the SOP's operating procedures should also apply to the operations of private sector computer security incident response teams to ensure uniformity of process and ease of presentation of evidence in court.

Special procedures will be necessary as the investigative procedures provided for in Chapter 2 of the CPA 51/1977 not sufficient when it comes to procedures to investigate cybercrimes/dealing with electronic evidence.

b) Telkom understands that:

- the law on the conduct of search and seizure operations be respected.

- that search warrants will be served with due regard to the rights of individuals and the businesses to avoid interference with infrastructure and networks that can disrupt communications.

Reply:

SAPS supports a process of consultation prescribed for the SOP's.

SAPS is in favour of preservation orders since no mechanism such as this exists in current legislation. This mechanism is necessary to preserve evidence, also in respect of requests received from foreign law enforcement agencies. Numerous of these requests are received, followed up by mutual legal assistance requests which creates a challenge since preservation orders is not yet part of our domestic law.

VODACOM

Submission:

Assisting police official or investigator

Clause 34 … must provide **technical assistance and other assistance** to a police official who is authorised in terms of a warrant to conduct an investigation, in order to search for/access/seize an article-

- Failure to comply can result in a conviction and a fine or imprisonment.

Vodacom proposes an amendment to clause 34(1) to include that in the instance where an article which is under the control of an electronic communications service provider, is subject to a search authorised in terms of clause 27(1), such search, access or seizure should be exercised in a way **which must not disrupt the services performed** by an ECSP.

Reply:

Clause 34: (assistance to police official during search and seizure by person suspected to be involved or who is in control of system that is subject to investigation).

Vodacom proposes that where an article is under the control of an ECSP and such article is seized it must not disrupt the services by a service provider.

This is in line with MTN's proposals.

First Rand is of the view that this provision should also provide for an objection clause by a system owner.

These concerns can be raised during the consultation process to formulate Standing Operating Procedures.

VODACOM

Submission:

Expedited Preservation Orders for Data/ Evidence.

Where data preservation orders are received that carry a "**Top Secret**" classification, such orders can only be dealt with by individuals that have the appropriate clearance.

Vodacom is concerned that it might receive preservation orders where the information requested would necessitate the involvement of individuals that do not have the prerequisite clearance levels.

Reply:

This submission is unfounded.

A classified order will not be served on any entity, since classification will make it un-implementable.

VODACOM

Submission:

Clause 54: (Obligations of electronic communication service providers/ financial institutions to report certain cybercrimes to the SAPS within 72 hours after becoming aware of such offences).

Vodacom is concerned about the workload and costs implied by this provision as well as the requirement to preserve "**any information**" which may be of assistance to law enforcement.

Vodacom submit that **"any information" must be specified.**

Reply:

It is not possible to foresee all possible information that may become relevant during an investigation.

An attempt to define all possibilities will, in SAPS's view, be impossible.

General comments

Clause 32(2) and clause 33(3) of the Cybercrimes Bill **do not allow the SAPS to, without a warrant, access a computer data storage medium** in **unique and urgent** circumstances, e.g. where a cellular phone is picked up on a crime scene and the SAPS is in pursuit of a fleeing suspect. It will be very challenging for the SAPS to obtain a warrant or even to apply for a warrant orally in circumstances where time is of the essence to prevent or to resolve an unfolding crime and the SAPS do not know what information is stored on the device or even to whom the device belongs.

The definition of a specifically "designated police official" in clause 1 should read as follows:

"*Means a member of the SAPS with the rank of Captain (instead of commissioned officer) or higher who has been designated by the National Commissioner and the National Head of the Directorate, respectively*…".

HAWKS
DIRECTORATE FOR PRIORITY CRIME INVESTIGATION

THANK YOU