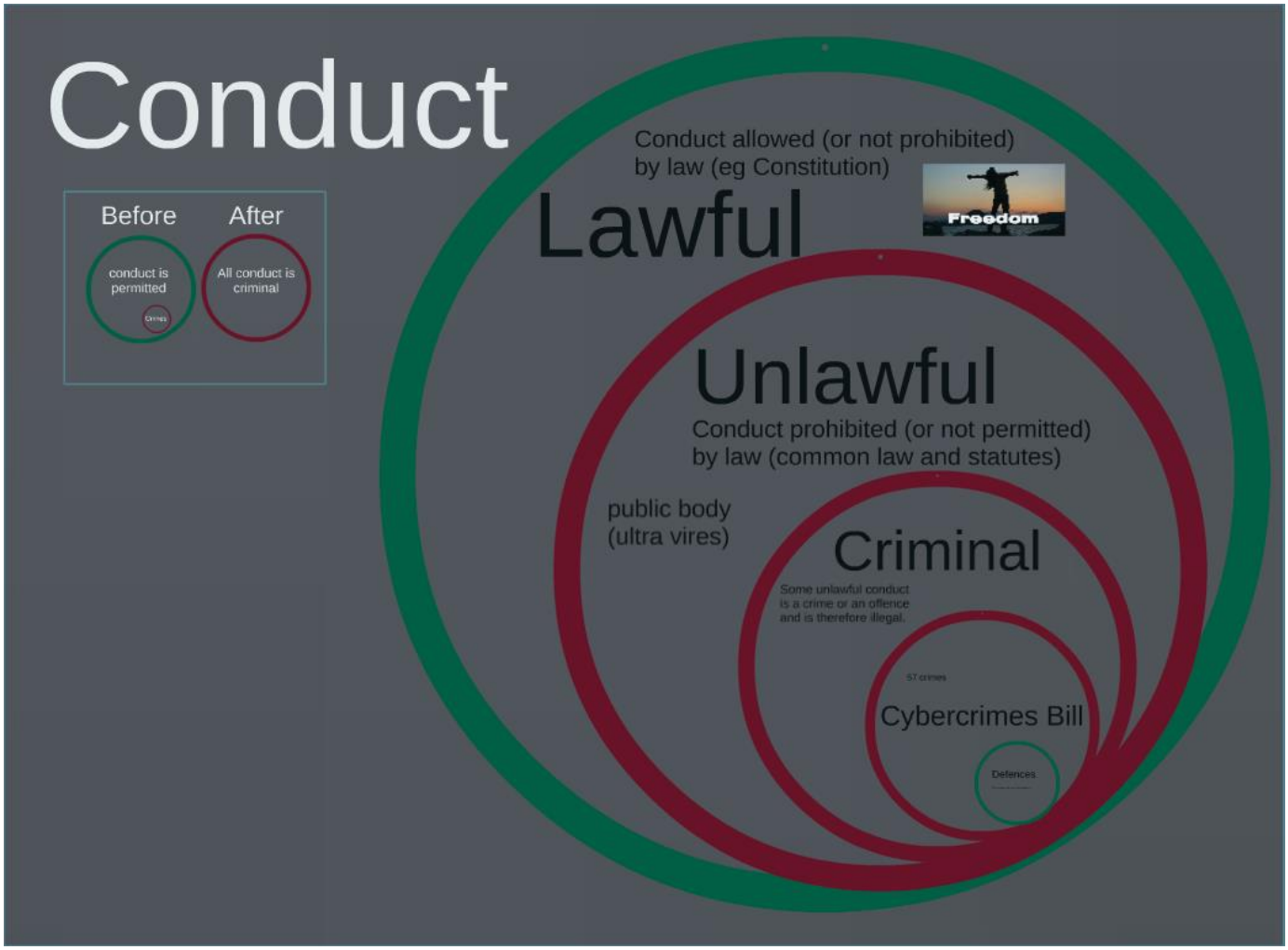
www.michalsons.com
support@michalsons.com
t. 086 011 1245
f. 086 529 4276
F5, Westlake Square, Westlake Drive, Westlake,
Cape Town, 7945
PO Box 260, Muizenberg, 7950

Comments on Cybercrimes and Cybersecurity Bill (B-6, 2017)

Introduction

We are Michalsons, a group of attorneys that specialise in ICT-related legal issues. We focus on various aspects of ICT, including data protection and cybersecurity. We have written extensively on Bill and its effect on our website: michalsons.com. We will comment on three parts of the Bill, namely: Chapter 2, Chapter 3 and Chapter 9.

Comments on Chapter 2 and 3 of the Cybercrimes and Cybersecurity Bill



Unlawfulness means conduct (or a consequence) that is prohibited by law. Broadly speaking, law is made up of common law and statute. What makes something unlawful is determined by a standard of objective reasonableness based on the legal convictions of society. In the post Constitutional era, the legal convictions of society are informed by constitutional values.

In the image above, lawfulness is the broad concept. It is essentially conduct that is allowed and not prohibited by any law. Unlawfulness, means conduct that is prohibited by the law, and some unlawful conduct is deemed to be a crime or an offence in certain cases, thus making that unlawful conduct illegal. In terms of the wording in the Bill, and the way the offences are drafted in Chapter 2, something is an offence only when you 'unlawfully' and intentionally do x. Essentially what this means is that if your unlawful conduct is unlawful, you are committed an offence in terms of the Bill. This understanding is circular and on the face of it, does not make sense.

Current clause in the Bill

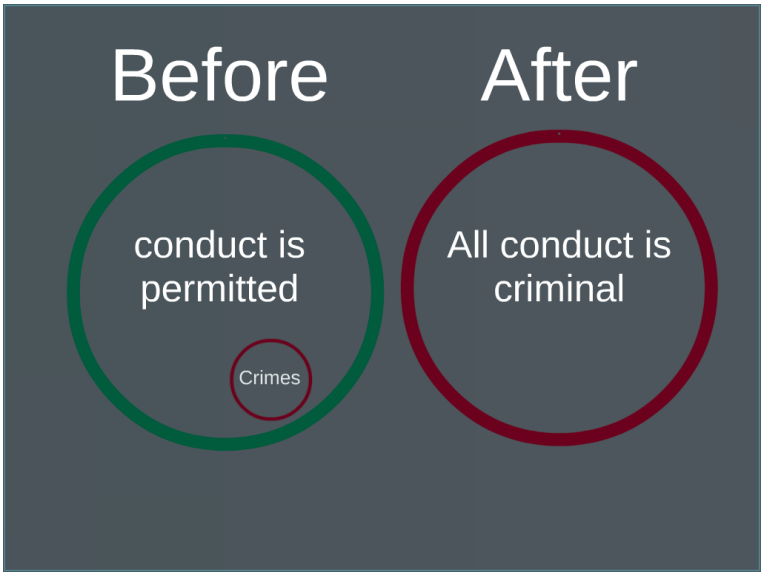
> *Unlawful securing of access*
>
> *2. (1) Any person who **unlawfully** and intentionally secures access to—*
>
> *(a) data;*
>
> *(b) a computer program;*
>
> *(c) a computer data storage medium; or*
>
> *(d) a computer system,*
>
> *is guilty of an offence.*

This section says that if I unlawfully and intentional secure access to data, for example, I am guilty of an offence. But for something to be an offence, the conduct must already be unlawful, and this conduct is unlawful as it is prohibited by this Bill. By simply adding the words 'unlawful' to every offence in the Bill, it creates a conundrum that could easily.

Another unfortunate effect of this broad wording is that unlawful conduct that was previously not a crime, is now a crime in terms of the Bill. For example, in section 9 of the Protection of Personal Information Act, 4 of 2013 (POPIA) you are required to lawfully process personal information. To lawfully process personal information, you must comply with the conditions set by POPIA. If you do not comply with those conditions, you are processing personal information unlawfully, but you are not committing a crime. POPIA defines processing to essentially mean doing anything with personal information. Considering the broad wording of the Bill however, your unlawful conduct of not complying with POPIA, could result in you committing a crime in terms of the Bill. POPIA was never intended to criminalise such conduct, otherwise Parliament would have made unlawful processing a crime in POPIA. If we refer to the image above, the unlawful processing in terms of POPIA places you in the red 'unlawful' circle. But because of the Bill, you would now be in the red 'Cyberrcrimes Bill' circle, which is inside of the 'criminal' circle.

Suggested amendment

Remove unlawfully from every offence in the Bill. Comparative legislation such as the Budapest Convention and the Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA) –Computer Crime and Cybercrime: SADC Model Law 2013, do not include the word 'unlawfully' when describing the various crimes.



The second image relates to the wording of the offences in the Bill.

In general, most conduct is permitted, and only some specified conduct is deemed to a crime. Most of the crimes in the Bill are too broadly defined, and the result is most if not all conduct is deemed to be criminal.

Current clause in the Bill

Unlawful securing of access

2*. (1) Any person who unlawfully and intentionally secures access to—*

(a) data;

(b) a computer program;

(c) a computer data storage medium; or

(d) a computer system,

is guilty of an offence.

(2) For purposes of this section a person ***secures access to****—*

(a) data when the person is in a position to—

(i) ***alter, modify or delete*** *the data;*

(ii) ***copy or move*** *the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;*

(iii) ***obtain its output*** *data; or*

(iv) otherwise ***use*** *the data;*

Unlawful acquiring of data

3. *(1) Any person who unlawfully and intentionally—*

(a) overcomes any protection measure which is intended to prevent access to data; and

(b) acquires data, within or which is transmitted to or from a computer system, is guilty of an offence.

(4) For purposes of this section, ***"acquire"*** *means—*

(a) ***use;***

(b) examine or capture data or any output thereof;

(c) ***copy*** *data;*

(d) ***move*** *data to—*

(i) a different location in a computer system in which it is held; or

(ii) any other location; or

(e) divert data from its intended destination to any other destination.

Unlawful interference with data or computer program

5. *(1) Any person who unlawfully and intentionally interferes with—*

(a) data; or

(b) a computer program,

is guilty of an offence.

(2) For purposes of this section, ***''interference with data or a computer program''***

means to permanently or temporarily—

(a) ***delete*** *data or a computer program;*

(b) ***alter*** *data or a computer program;*

(c) render vulnerable, damage or deteriorate data or a computer program;

(d) render data or a computer program meaningless, useless or ineffective;

Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices

7. *(1) Any person who unlawfully and intentionally—*

(a) ***acquires;***

(b) possesses;

(c) provides to another person; or

(d) ***uses,***

a password, an access code or similar data or device for purposes of contravening the provisions of section 2(1), 3(1), 5(1), 6(1), 8 or 9(1), is guilty of an offence.

Above, we have quoted four different clauses in the Bill. At first glance, these clauses all relate to distinct and separate crimes. However, when we examine the definitions further, there are many overlaps and it is unclear what conduct the clauses are criminalising.

For example, 'securing access' in clause 2, and 'acquire' in clause 3 both have overlapping meanings. Both include use of data in their definition. Both include moving and copying in their definition. Further, 'interference with data or a computer program' and 'securing access' both include deleting or altering in their definition. There it is unclear what is different and distinct in the clauses, and what specific conduct the clauses deal with. Essentially what this means is that if you do anything with data or a computer program that is deemed to be unlawful, is committing an offence.

If we look at unlawfulness broadly, it must be seen in terms of the concept of legality. The criminal justice system uses arrest, trial and punishment and these means interfere with civil

rights. Those interferences are permitted in certain circumstance but are moderated by the rule of law and the Bill of Rights. Legality is essentially the rule of law in the context of criminal law.

The basic principle of legality is punishment may only be given for the contravention of a clearly defined crime that was created by law which was in force before the contravention. The principles of legality were common law principles (and remain so) but they are also in the Constitution s 35(3)*(l)* to *(n)*.

A key aspect to the principle of legality states that common law and statutory crimes must be defined with reasonable precision. This principle is in the Constitution in s 35(3)*(a)* the right to be informed of a charge in sufficient detail to be able to answer it. Further, vaguely worded crimes infringe the right to a fair trial.

The crimes in the Bill are not worded with reasonable precision. As shown above by the quoted clauses, there is significant overlap in the definitions of the crime because the crimes are drafted so broadly, and vaguely. One could be charged for multiple crimes simply based on the overlaps.

Defences

There is a relationship between unlawfulness and defences that exclude unlawfulness. Essentially, a person might have done the act prohibited by law but may escape liability by raising a defence that excludes unlawfulness. The existence of these defences is based on the theory that the same society that deems the conduct to be in contravention to their values but also deemed it justified conduct in certain circumstance.

Current clause in the Bill

The clauses in the Bill do not have any defences except in one circumstance:

> *Unlawful securing of access*
>
> *2. (1) Any person who unlawfully and intentionally secures access to—*
>
> *(a) data;*
>
> *(b) a computer program;*
>
> *(c) a computer data storage medium; or*
>
> *(d) a computer system,*
>
> *is guilty of an offence.*
>
> *(2) For purposes of this section a person secures access to—*
>
> *(a) data when the person is in a position to—*
>
> *(i) alter, modify or delete the data;*
>
> *(ii) copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;*
>
> *(iii) obtain its output data; or*
>
> *(iv) otherwise use the data; …and the access contemplated in paragraph (a), (b), (c) or (d) which the person secures is* ***unauthorised.***

Suggested amended clause

> *2. (1) Any person who ~~unlawfully and~~ intentionally and without authorisation* [OR] *without any justification ~~secures~~ accesses ~~to~~—*
>
> *(a) data;*
>
> *(b) a computer program;*

(c) a computer data storage medium; or

(d) a computer system,

is guilty of an offence.

(2) For purposes of this section a person secures access to—

(a) data when the person is in a position to—

(i) alter, modify or delete the data;

(ii) copy or move the data to a different location in the computer data storage medium in which it is held or to any other computer data storage medium;

(iii) obtain its output data; or

(iv) otherwise use the data; ~~…and the access contemplated in paragraph (a), (b), (c) or (d) which the person secures is unauthorised.~~

We suggest adding 'without authorisation' or 'without any justification' to that clause and to the other offences in the Bill, similar to the above.

Reverse Onus

Unlawful acquiring of data

3. (1) Any person who unlawfully and intentionally—

(a) overcomes any protection measure which is intended to prevent access to data; and

(b) acquires data, within or which is transmitted to or from a computer system, is guilty of an offence.

(2) Any person who unlawfully and intentionally possesses data, with the knowledge that such data was acquired unlawfully as contemplated in subsection (1), is guilty of an offence.

*(3) **Any person who is found in possession of data, in regard to which there is a reasonable suspicion that such data was acquired unlawfully as contemplated in subsection (1) and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.***

In terms of a reverse onus, in S v Zuma 1995 (2) SA 642 (CC), the Constitutional Court stated that not all statutory provisions that create a reverse onus are unconstitutional (because they unjustifiably infringe on the presumption of innocence). The court will weigh up factors relating to the social need for the successful prosecution of crime. The concerns with reverse onuses is not whether the accused must prove an excuse or disprove an element but rather that reverse onuses can create a situation where the accused could be convicted where reasonable doubt exists. Where that probability exists, there is a breach of the presumption of innocence (reworded from S v Zuma).

Comments on Chapter 3 of the Cybercrimes and Cybersecurity Bill

S18 - Current Clause

18.(1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of an identifiable person knowing that the person depicted in the image did not give his or her consent to the making available, broadcasting or distribution of the data message, is guilty of an offence.

(2) For purposes of subsection (1), "intimate image" means a visual depiction of a person made by any means—(a)under circumstances that give rise to a reasonable

expectation of privacy; and(b)in which the person is nude, is exposing his or her genital organs or anal region or, in the case of a female, her breasts

S18 – Suggested amended clause

18. The non-consensual, creation, possession, solicitation, publication or distribution of any data message, however created, or any description of a person, real or simulated, showing or describing the body, or parts of the body, of such person in a manner or in circumstances which, within the context, violate or offend the sexual integrity or dignity of that person

Motivation for changes

We feel that limiting the clause to only cover nudity is insufficient. Frequently revenge porn can include pictures or descriptions that do necessarily depict the victim fully nude, but can be equally damaging to their dignity. As an example, “cum shots” (a picture of a person, frequently a woman with male ejaculate on her face or other body parts) as they are referred to would not be covered. The amendment proposes that what constitutes as revenge porn should be wider to include these sorts of pictures or descriptions as they equally as damaging.

We also feel that the need to have the person “identifiable” is too limiting. Our reading of this section proposes that the data message itself must be able to identify the victim which is insufficient to protect victims. Frequently revenge porn will not have identifiable marks or even be depictions of the actual victim, but is depicted in a context or with additional information that is intended to make the recipient of the message believe it is the victim. Our proposed change will cover this eventuality.

Lastly, we believe that the “reasonable expectation of privacy” limitation is unjustified. There have been several cases where revenge porn is captured in “public” areas and typically where the victim is in some way compromised (drunk, or under the influence of narcotics). It also needs to cover the eventuality that the victim may have consented to the creation of the data message (and even intended for it to be distributed) but then changes their mind.

While we appreciate the need for creation of a crime of this nature, we would propose that it should be contained in the Sexual Offences Act and not here.

S17 – Current Clause

17.(1) Any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which is harmful, is guilty of an offence.

(2) For purposes of subsection (1), a data message is harmful when

—(a)it threatens a person with

- (i) damage to any property belonging to, or violence against, that person; or

- (ii) damage to any property belonging to, or violence against, any member of the family or household of the person or any other person in a close relationship with the person;

(b)it threatens a group of persons with damage to any property belonging to, or violence against, the group of persons or any identified person forming part of the group of persons or who is associated with the group of persons;

(c)it intimidates, encourages or harasses a person to harm himself or herself or any other person; or

(d)it is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm to a specific person or a group of persons, and a

reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful.

S17 – Suggested Addition

Subsection 2(d) is problematic as it potentially criminalises satire, parody or artistic or other works that are intended to be used as political commentary. We would like to see the inclusion of a defence for works of this nature.

Comments on Chapter 9 of the Cybercrimes and Cybersecurity Bill

Current 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 subsection (2), must—

(a) 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*

(b) ***preserve any information*** *which may be of assistance to the law enforcement agencies in investigating the offence.*

This clause requires an ECSP or financial institution to report an offence to the Police when it becomes aware or is aware its computer system is involved in the commission of any category or class of offences provided for in Chapter 2. It is not clear if they should only report an offence is the crime is being committed against their computer system or if their computer system is being used to commit an offence.

(2) The Cabinet member responsible for policing,

Section 47(2): This subsection requires Electronic Communications Service Providers (ECSPs) to immediately report an offence in terms of the bill when they are aware or become aware that a computer is involved in such an offence. Further, the clause does not consider that the ECSP or financial institution may have its own internal incident response policy that deals with this situation. For example, it does not consider that an ECSP may not want to broadcast that they have had a breach in their systems especially if they have not had the opportunity to address it internally and fix it, before they report it to the police. There is a big risk to an ECSPs' reputation especially if they have to report every single incident.

Reporting should take place after their have exhausting their internal policies to deal with the issue and reporting to the Police should not be required for every single circumstance. High priority incidents should be reported to the Police. Incidents that can be dealt with internally, should not be required to be reported. This reporting section should consider section 22 of POPIA which deals with the notification of security compromises. S22(2) states that notification must be made "as soon as reasonably possible after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system." This approach allows the ECSP or financial institution to implement its internal incident response policies. The clause should be rewording to considering these POPIA requirements.

The GDPR's (the European Union's General Data Protection Regulation's) approach should also be considered. Article 33(1) deals with notification of a personal data breach to the supervisory authority. It states that a breach should be reported "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." Similar to the previous paragraph, a risk-based approach should be taken, so that the Police are not overrun with ECSPs and financial institutions reporting every single incident to them. An ECSP or financial institution should be allowed to give reasons should they not report an incident with 72 hours. There should also be a possibility of an extension to the time period.

The clause also requires ECSPs or financial institutions to preserve any information that can assist in an investigation. This is not feasible, especially as the information may be located in various forms such as servers, cloud storage etc. Storing that amount of information for an unspecified time is not realistic. A time period should be put in place so that ECSPs or financial institutions are not holding the information for indefinite period. The Minister of police must also prescribe how long ECSPs or financial institutions must preserve data necessary to assist in investigations.

The fine in clause 52(3) does not consider the size of the organization and whether the amount would be feasible for small ECSPs or irrelevant to large ones. The fine should be a percentage of annual turnover (like the mechanism in the GDPR).

Closing remarks

John Giles and Lisa Emma-Iwuoha of Michalsons, would gladly make ourselves available to give oral comments on the Bill during the public hearings.