Information Governance Consulting
in collaboration with MARK HEYINK

3 Heron Avenue
Dowerglen 1609

eMail: mark@heyink.co.za

Telephone: (27 11) 454-0449
Fax: (27 11) 454-0036
Mobile: 082 904-3774

BY E-MAIL TRANSMISSION

THE PORTFOLIO COMMITTEE ON
JUSTICE & CORRECTIONAL SERVICES
eMAIL: vramaano@parliament.gov.za

08 August 2017

Your ref: Mr V Ramaano
Our ref: Mark Heyink

Dear Sirs,

SUBMISSIONS ON THE CYBERCRIMES AND CYBERSECURITY BILL

1. My name if Mark Heyink. I am admitted attorney, notary and conveyancer of the High Court of South Africa and practice as such under Mark Heyink Information Attorney. In addition to my legal qualifications I have studied Information Management at the Wits Graduate School of Business and qualified as a Certified Information Systems Security Professional in 2006. Supplementary to the services provided through my legal practice I am a director of Information Governance (Pty) Limited that provides consultancy services relating to the governance, management and security of information and communications technologies and the information processed using these technologies.

Credentials

2. In 2002 I was engaged by KPMG to, on behalf of a large number of its clients, submit representations on the Electronic Communications and Transactions Bill. In doing so I convened and chaired a number of workshops attended by subject matter experts and clients of KPMG. I drafted the joint submissions of the clients to the Parliamentary Portfolio Committee of Communications (as it then was). These submissions formed the most comprehensive comment that was provided on the Bill.

3. In 2002 I was appointed by the then Minister of Justice of the South African Law Reform Commission tasked with the research of privacy law and the drafting of a bill known as the Protection of Personal Information Bill. This was submitted to the Minister of Justice at that time together with the report of the South African Law Reform Commission. After the Minister's approval the report was published and submissions on the Bill were invited. I responded by providing written submissions and oral recommendations to the Parliamentary Portfolio Committee for Justice. I was then requested by representatives of both the African National Congress (the Honourable John Jeffery) and the Democratic Alliance (the Honourable Dene Smuts) to assist the Joint Portfolio Committee in its deliberation and finalisation of the Bill before its enactment.

4. Between 2009 to 2013, I attended all of the meetings of the Technical Committee appointed by the Joint Portfolio Committee and the meetings of the Portfolio Committee and save for one, all of the meetings of the Portfolio Committee in its deliberation on the Bill, until its eventual enactment in 2013. I did this as a private citizen and was not paid for my services nor the costs of travelling to and from Johannesburg and my accommodation while in Cape Town.

5. On the 10th February 2015, in the absence of an Information Regulator (which had not been appointed at that time), I attended the Parliamentary Portfolio Committee meeting for Finance to address what I believe is an unlawful provision in the Financial Services Regulatory Bill. These provisions circumvent the powers of the Information Regulator and require to be addressed. I did this at my own cost.

6. I have served as an advisor on the National Cybersecurity Advisory Council established to advise the Minister of Telecommunications and Postal Services. My term of office expired in March of this year.

7. Since 2015 I have been in liaison with the drafters of the Cybercrimes and Cybersecurity Bill and the Deputy Minister of Justice relating to numerous aspects of the Bill. I have served on the Expert Committee convened by the Deputy Minister of Justice.

Socio-economic Importance of the Information Revolution

8. It is an indisputable fact that we are in the midst of an information revolution founded on the use of the internet and mobile technologies that has fundamentally and irretrievably changed our interactions, socially, economically and politically. It is recognised that these changes, if taken advantage of, can be hugely beneficial to the wellbeing of our society. The changes have also heralded abuses that are currently not addressed in our law. Indeed, one of the purposes of the Cybercrimes and Cybersecurity Bill ("the Bill") is to address some of these abuses.

9. However, in the same way that the novel applications of the technologies have had to be approached differently from how we may have approached their equivalent in the paper and text world, so too does the law in this regard hold fundamental differences in approach that cannot be ignored. Unfortunately, this has not been properly appreciated in the drafting of the Bill to date.

10. It must also be recognised that the role of government relating to our information society and economy, both legislative and administrative, needs reconsideration. While government should play a leadership role, the significant differences in our information society and economy from what was previously the case needs to be addressed if the law is to be practical and effective. In this regard the context of the capacity and capability of government to fulfil its obligations has to be taken into account in dealing with prospective legislation in the cyber realm.

Information or Cybersecurity within Government

11. Turning to the issue of cybersecurity within government, the Minister of State Security has made several pronouncements in this regard. One of these is:

"It has consistently been the position of the government that we recognise the importance of the technological advancements and potentially moving our country forward."

The Minister adds:

"My department is essentially the security risk manager of SA Inc. and therefore cannot sit idly by when the advancement in technology presents both opportunities and threats which we have to appraise the government of."

12. While recognising the responsibilities of his department, the Minister fails to take account of his own department's failure to fulfil these responsibilities. By way of example. It is not entirely clear what the real status of the Minimum Information Security Standard (MISS) is. The general understanding, however, is that this is the responsibility of the State Security Agency. MISS was published in 1996. It was already inadequate in 1996 to deal with emerging technologies and the protection of information in digital form. The fact is that information security within government is typically poor.

13. A further fact is that draft information security regulations were prepared as long ago as 2005. These draft regulations incorporated best practice recognised in international standards around the world. They constitute a quantum leap from the inadequacy of MISS, yet they have never seen the light of day. The question that must be considered and answered is who is responsible for information or cyber-security within government? With great respect the structuring in the Bill is not clear on who will be responsible and accountable for information or cyber-security failures.

14. Whatever policy may exist within government relating to information and communications technologies, cybersecurity and cybercrime, it remains fragmented.

15. The Committee is urged in considering the structures proposed in the Bill to investigate whether they are indeed practical and that the skills required to implement some of the noble intentions contained in the Bill are available to government. The Committee is also urged to clarify responsibilities and accountability for cyber security and policies supporting cybersecurity.

16. The observations relating to policy, capability and capacity failures that have undoubtedly occurred in the past, cannot be confined to the ruling party. None of the opposition parties have evidenced any meaningful interest in developing informed policy relating to cybercrime or cybersecurity.

17. All of the parties on the Committee are strongly urged to take very seriously the proposed legislation. Addressing cybercrime and cybersecurity is critical to the future well-being of South Africans and demands time, effort, consideration, and possibly acceptance, of thinking that has not necessarily characterised law-making in the past.

CYBERCRIMES AND CYBERSECURITY BILL

Issues of Principle

18. In dealing specifically with the Cybercrimes and Cybersecurity Bill there are several issues that must be addressed. First and foremost is the necessity to be honest with ourselves and one another.

19. The requirement of honesty will require a maturity in approach that encompasses the involvement of all South Africans and the use of the limited resources at our disposal, wisely. The development of expertise and the capacity necessary to take advantage of the enormous benefits that the information revolution holds for South Africa and to protect against abuses, should be a National Imperative. This is not a sphere in which party-political agenda will be helpful. It requires a concerted effort and strong political will that has, to date, been absent. Without this cooperative and inclusive approach it does not matter what legislation will be passed, it is doomed to failure.

Separation of Cybercrimes and Cybersecurity

20. A number of representations have been made calling for the splitting of the Bill into two parts. There should be a Cybercrime Bill and a Cybersecurity Bill. Cybercrime is the domain of the Department of Justice. Cybersecurity on the other hand, while the State Security Agency has an important role to play, encompasses a broader spectrum within government and meaningful engagement with the private sector that needs to be considered on that basis. With the greatest respect, the very broad ambit of cybersecurity falls outside of the exclusive remit of this Committee.

21. Should this Committee not agree with this sentiment it must take cognizance of the fact that the provisions of the Bill as it stands address cybersecurity responsibilities without addressing the proper coordination of a cybersecurity framework across both the public and private sectors. Cooperation and co-ordination of cybersecurity across all sectors of society is a characteristic of cybersecurity legislation in democracies globally.

UNDERLYING DRAFTING ISSUES

In the process of the drafting of the Bill, three major observations were brought to the attention of the Department of Justice. These were:

Consultative Process

22. The normal research and consultative process that would characterise legislation of such broad application has not been followed. This failure has led to the Bill being heavily biased towards national security and law enforcement at the expense of civil liberties. Whoever may be in power may use this bias to abuse the civil liberties of citizens and lead to selective prosecution. This trap must be avoided in any democratic society.

23. This is exacerbated by the broad terms used in the drafting being subject to many different interpretations. In this regard I have, in the extensive consultation that I have had with lawyers skilled in this area and experienced hours of debate as to what the drafters actually meant in some of the clauses. As the Bill will affect all citizens across a wide spectrum of our society the failure to draft the Bill in plain language and terms that is easily understandable by the many people that will be affected by the Bill, is highly undesirable and dangerous in a democracy. If skilled lawyers cannot understand the Bill what chance does the layman have?

24. The Committee is urged to encourage openness and a vigorous consultative process its consideration of the comments provided to it relating to the Bill. While the legislation is long overdue its importance to the future of on-line South Africa cannot be underestimated.

Public/Private Partnerships

25. Unlike frameworks that have been developed in other countries relating to cybercrime, where cooperation between the private and public sectors is seen as key to cybersecurity, the Bill takes an authoritarian approach to cybersecurity.

26. The provisions of Chapter 11 dealing with National Critical Information Infrastructure must engender public private partnerships which despite being addressed in the NCFP are strangely absent from the Bill. The committee must take cognisance if the fact that much of our Critical Information Infrastructure is owned and operated by the public sector.

27. The document entitled the "Minimum Information Security Standard" (MISS) still regulates information security in government departments, despite it not having been amended since 1996. This is outdated and must be replaced with a more inclusive approach. Certainly the approach to cybersecurity must be more creative than what is contemplated in MISS and used by the State Security Agency as a benchmark within government.

Privacy and the Protection of Personal Information

28. In democracies around the world it is well-recognised that the counterbalance to overzealous government and unscrupulous business in our information society is the right of privacy. In South Africa, this is a constitutional right entrenched in the "Bill Of Rights". The growing importance of privacy is illustrated in the efforts of governments around the world to protect privacy. In the European Union the implementation of the General Data Protection Regulations (GDPR) applicable to all European Union members, serves to enhance the protection of personal information. The GDPR is the gold standard against which the protection of privacy and of personal information will be judged.

29. The status of the protection of our right of privacy and privacy in our personal communications and information and particularly its close relationship to cybersecurity, remains regrettably uncertain and misunderstood. The following summary may be of assistance to the Committee.

30. The Bill of Rights provides that:

> *"Everyone has the right of privacy, which includes the right not to have - …*
>
> *(d) The privacy of their communications infringed;"*

31. The Protection of Personal Information Act states among its purposes:

> *"Give effect to the constitutional right of privacy, in safeguarding personal information processed by a responsible party, subject to justifiable limitations aimed at: …*
>
> *(i) Balancing the right of privacy against other rights; …*

(b) Regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for lawful processing of personal information; …

(d) Establish voluntary and compulsory measures, including the establishment of an information regulator, …"

32. The issue of information security or cybersecurity is closely linked to the protection of personal information ("data protection" legislation as it is referred to in some other jurisdictions). The emergence of modern technologies allowing for the processing of vast volumes of information as well as ease of its communication, has resulted in abuses on the part of overzealous government and unscrupulous business. Global debate relating to the balance between privacy and security is the most prominent jurisprudential debate that exists in this early part of the 21st century. With respect the Bill does not take into account the status of privacy and protection of personal information into account as it undoubtedly should.

33. It is unfortunate that although the Information Regulator has now been appointed and the global acceptance that good privacy law, properly implemented and monitored by an independent regulator, provides a balance against overbroad security laws, the operative portions of the Bill have not yet been proclaimed to commence.

34. It is also a fact that in countries that have mature data protection legislation, cybersecurity is much better than in those that do not have data protection or protection of personal information legislation. This is not surprising as, as the name suggests, the "protection" of data or information requires information security and the fact that this has not until recently been legislated in South Africa (as opposed to other countries where it has been part of the legislative landscape for excess of 25 years), has led to South Africa having an inferior and weak cybersecurity posture.

35. The Committee is strongly urged to investigate this issue. It will find that cybersecurity frameworks established in democracies are characterised by the balance provided by data protection or privacy laws. In fact, the "African Union Convention on Cybersecurity and Personal Data Protection", which informed some of the drafting of the Bill, deals with both issues and emphasises the importance of data protection. The importance, however, of privacy and the powers of the Information Regulator has not been recognised in the Bill that has failed to take account of the novelty of this law in the socio-economic fabric of our 21st century society. *Emphasis added by the author

36. What is important to take into account is that the Information Regulator has yet to become properly operative and in a position to allow the President to proclaim the commencement of operative provisions of PoPIA.

37. Against this background the Committee is urged to recommend that fresh attention is paid to the Information Regulator, the proclamation of commencement of the provisions of the Protection of Personal Information Act and the relationship between the law governing privacy and the Bill.

38. Should the Committee fail to do so (particularly in light of the expertise and capacity restraints that have been highlighted relating to cybersecurity) it may render to the powers conferred by the Bill as it stands, unconstitutional.

ORAL COMMENT AND SUBMISSIONS

I request that I be afforded the opportunity of making oral comment to the Committee and look forward to receiving details of the time and date that these may be heard.

Kind regards,

Yours sincerely
MARK HEYINK