PREFACE TO COMMENT ON CYBERCRIMES AND CYBERSECURITY BILL ("the Bill")
Prepared by Mark Heyink 12th November 2015

Importance of cybersecurity legislation

South Africa, like many other countries, is subject to the disruption of our social-economic and social-political circumstances by the rapid development of novel technologies and their application in our society. It should immediately be recognised that the technologies are neutral, typically they create opportunities as technologies are developed to unlock the potential to benefit persons within our society. However, they can be and are abused. In some instances the harm caused is motivated by greed, but as often the harm lies in the abuse of the technologies to gain power and influence.

Against this background the development of appropriate cybercrimes and cybersecurity legislation is essential. Since 2002 when the Electronic Communications and Transactions Act 25 of 2002 ("ECT Act") was debated and enacted, which Act created the first cybercrimes, it was recognised that the ambit of the crimes in the ECT Act were too narrow. Against this background, since 2002 laws relating to cybercrimes and cybersecurity has been agitated for in certain quarters, but these pleas have largely been ignored. The unfortunate fact is that despite having been a signatory to the European Union Convention on Cybercrime since 2002, little has been done by government for the past 13 years to address this critical issue. What has been done has unfolded at a glacial pace despite the rapidly accelerating cybercrime and cybersecurity threats that our information society faces.

An indication of the inertia of government in this regard lies in the fact that the Bill has as its genesis the National Cybersecurity Policy Framework (NCPF) for South Africa. This framework was first published in 2010 in draft form. It was finalised and signed off by Cabinet in 2012 but remained classified until very recently. In fact, despite it being foundational for the Bill, it was only declassified halfway through the period between its publication for comment and the deadline date for comment to be provided. The National Cybersecurity Implementation Plan also remains classified at this time. Just another example of the blundering of the JCPS Security Cluster in dealing with this legislation, despite its importance and the urgency that current circumstances demand.

It should also be noted that the Minimum Information Security Standards (also known as MISS), which governs information security measures within government, was first published in 1996 (almost 20 years ago). Despite the dramatic shifts in how information is communicated and processed in government, MISS, an anachronism for many years, has never been amended or replaced. Despite draft Information Security Regulations being around for many years, they remain classified and have not seen the light of day. Unfortunately, what this tells us is that even while it is stressing the urgency of cybersecurity on the one hand, government has been regrettably (and possibly even unforgivably) lax in establishing appropriate information security structures within its own administration.

Despite the necessity to address the issue of cybercrime and cybersecurity (two wholly separate issues the wisdom of dealing with both issues in one piece of legislation must be questioned), this issue has been largely ignored by government for years, and now suddenly, with seemingly indecent haste, it seeks to enact legislation which holds important implications for our future information society without properly and diligently examining the implications thereof.

There are three critical issues of principle which I address in this preface that influence my comment on the draft legislation as it stands. These are:

- The approach to drafting the Bill and failures of proper consultation;
- The failure to recognise the importance of public/private partnerships; and
- The failure to balance the constitutional rights of citizens, the powers of law enforcement and national security agencies.

Approach to drafting and failures of proper consultation

It must be recognised that this legislation emanates from the JCPS Cluster and it is in essence a product of the State Security Agency. While the drafting of the Bill has been conducted under the auspices of the Minister of Justice and Correctional Services, it is nonetheless directed by the NCPF, and is a product of the State Security Agency, essentially working in conjunction with other members of the JCPS Cluster. The Department of Justice has been given the responsibility of drafting the legislation.

With this is as a background it is not surprising that several aspects of the Bill reflect an unacceptable (and in certain instances unconstitutional) bias towards law enforcement and national security at the expense of civil liberties.

The drafting is not supported by appropriate research and information to allow for the ease of comment by parties considering the Bill. It has been drafted essentially by lawyers, without regard for the benefits of a multidisciplinary approach to the various issues that it addresses (in fact a single lawyer). This issue was raised in providing comment to a previous draft “The Cybercrimes and Related Matters Bill”. It would appear, in response to that, that a “Discussion of the Cybercrimes and Cybersecurity Bill” has been provided. Unfortunately, if the “Discussion of the Cybercrimes and Cybersecurity Bill” was intended to substitute proper research supporting the Bill, it fails dismally in doing so. For the most part it is simply a re-statement of provisions in the Bill in more user-friendly language with some very “high level” comment. The fact is that it betrays the drafter’s lack of understanding of how significant parts of information and communications technology infrastructure that the Bill addresses, actually work.

The question that must be raised is why the approach has been adopted as opposed to using the South African Law Reform Commission mechanisms? This would allow for a project committee to have been formed comprising experts and including expertise from both the public and private sectors to deal properly with the Bill and bring to bear the considerations that are important in legislation of this nature.

Surely in light of the fact that it is recognised that vast parts of the critical information infrastructure of our country is owned and controlled in the private sector, the involvement of private sector interests through a proper consultative process at the early stages of the drafting of this legislation would have been preferable, and, it is submitted, far more productive. Unfortunately, however noble statements of government may be, its actions deviate significantly from the sentiment and intent of the NCFP. If the Bill remains in its current form it will establish government control over ICT infrastructure that it has no right to control.

This is diametrically opposed to the guarantees afforded by the Constitution.

The failure to recognise the importance of public/private partnerships

Cybersecurity frameworks globally recognise that in most societies the critical infrastructure required to process information in both our information society and information economies is held in the private sector. The importance of creating public/private partnerships is stressed. This is reflected in the NCPF but this is not advanced into the Bill. While it is recognised that government has a leadership responsibility with regard to cybersecurity and that its role is to coordinate the efforts of the public and private sector in this regard, the concept of partnership is critical to this relationship.

The effect of the Bill is to place government in a dictatorial role as opposed to a leadership role and grants powers that are wholly inappropriate in addressing the interaction between private and public sectors relating to cybersecurity.

One of the unfortunate issues in this regard is that government itself has failed over many years to establish appropriate cybersecurity within the public sector and has hardly placed itself in a position to determine for the private sector how it should go about establishing appropriate cybersecurity measures. Its failure in this regard is aptly demonstration from the fact that MISS, a relic of the 20th century, remains operative in the vastly different circumstances of the 21st century.

The failure to balance the constitutional rights of citizens, the powers of law enforcement and national security agencies

The most disturbing element of the Bill is the absence of the appreciation, which is a feature of all credible cybersecurity frameworks, of establishing a balance between civil liberties and the powers of national security and law enforcement agencies. There is simply no acknowledgement of the constitutional right of privacy, which has been globally recognised as critically important in legislative frameworks that are being developed to address 21st century issues.

The revelations of Edward Snowden have highlighted the dangers of law enforcement and national security being overzealous in the exercise of their powers. The repercussions of this can be seen in the striking down by the European Court of Justice of the Safe Harbour Accord (intended to protect the privacy of personal information of EU citizens that is processed in the USA) as a result of law enforcement overreaching its powers. While it is lamentable that the Department of Justice and Constitutional Development have not acted expeditiously in ensuring the protection of the constitutional right of privacy has a meaningful place in our law (it being more than 13 years since it was regarded as urgent that this matter be addressed by the South African Law Reform Commission and that the Protection of Personal Information Act is still is not operative in this regard). The enactment of legislation as proposed in the Bill in the absence of privacy protections is out of line with all credible cybersecurity frameworks and is an assault on the civil liberties of South African citizens.

If we ignore the civil liberties of our citizens and institutionalise the powers of national security and law enforcement that are simply unconstitutional as currently provided in the Bill, we run the risk of being excluded from the greater information society and other 21st century economies, in the same way as the apartheid regime was ostracised for its apartheid strategies.

As Benjamin Franklin has observed:

> *"Those who give up their liberty for more security, neither deserve liberty nor security."*

Conclusion

Further comment on the Bill will support the general observations made on the Bill in this response. It must be recognised that as it stands there are many issues on the Bill that are ill-conceived, do not take account of the critical importance of the private sector in cybersecurity and the Bill is in several respects simply unconstitutional.

While the importance of establishing appropriate protections and ensuring that cybersecurity becomes a culture in our society is not only accepted but government has been urged to take action in this regard for years, this does not mean that the Bill should be rushed or ill-considered. There can be little doubt that as it stands, the Bill is strongly influenced by the State Security Agency and the JCPS Cluster and evidences a strong bias towards government control of the information and communications technology infrastructure of the country, at the expense of civil liberties of citizens.