



# SACF SUBMISSION ON THE CYBERSECURITY AND CYBERCRIMES BILL, 2017

Submitted on 10 August 2017

## **INTRODUCTION**

1. The South African Communications Forum (SACF) is an industry association and represents a broad cross section of participants in the Information and Communications Technology (ICT) sector. Our members include some of the leading stakeholders in the Telecommunication, Electronic Media, Postal, Information Technology, Electronic Manufacturing, OTT and Broadcasting Industries.
2. Our submission represents the views of our members and sets out key concerns of SACF members in a bid to make the Bill practicable as we are of the view that the Cybercrimes and Cybersecurity Bill (B6-2017) ("the Bill") is necessary to create a framework to comprehensively address Cybercrimes and Cybersecurity.
3. The SACF and its members welcome the Department of Justice and Constitutional Development's (DoJ@CD) consideration and incorporation of comments by our members in the previous draft of the Bill as submitted by some SACF members. As a result our comments on this draft are limited, to provisions that we are of the view that still need to be addressed.
4. The SACF would like an opportunity to make an oral submission on the Bill, should there be public hearings and participate in any further consultations in this regard.

## **GENERAL COMMENTS**

5. Our submission will thematically address the areas of key concern to our members, and members may submit detailed comments which may reflect their specific concerns.
6. The SACF and its members welcome the draft Bill due to the growing risk of Cybercrimes and the consequent need for cybersecurity. This is evidenced by the growing number of indiscriminate Cyberattacks which are less discerning between attacks on corporates and individuals.

7. A comprehensive, clear legislative framework is essential. It is as important to ensure that provisions of the legislation are forward looking crisp, simple and comprehensive to limit potential loopholes.
8. The Bill in the main sets out this framework.

## **OFFENCES**

9. Chapter 2 of the Bill sets out the cybercrimes, which we believe is largely aligned to international best practice. However, we note that the Bill inadvertently omits two key cybercrimes which in our view ought to be included due to the significance and magnitude of its consequences – these are identity theft and phishing. We therefore, propose that these are included in the Chapter 2 on Cybercrimes.
10. Identity theft otherwise known as identity fraud is often a building block for other cybercrimes as it misrepresents the identity of the person soliciting or conveying information which determines how the recipient of the message receives the message and the actions that follow. The consequences on the person whose identity has been stolen are potentially dire and the impact can be long standing.
11. We are of the view that identity theft is not adequately provided for in the list of cybercrimes included in the Bill and is a distinct crime and ought to be recognised as such. The SACF therefore proposes its inclusion in the Bill.
12. Phishing is the activity where information is fraudulently obtained using emails that misrepresent the entity requesting specific information by purporting to be a legitimate entity (individual or corporate) requesting relevant information for illicit purposes. It must be noted that there are multiple variants of phishing.
13. While, Clause 9 of Chapter 2 of the Bill, deals with cyber forgery, it does not expressly include phishing. Due to the extent and impact of phishing, we are of the view that this ought to be recognised as a distinct crime.

14. Consequently, we would urge the Department to include identity theft and phishing as distinct Cybercrimes in Chapter 2.

## **PENALTIES**

15. The SACF and its members are of the view that penalties must be proportionate to the magnitude of the impact of the crime. The maximum penalties provided for in Clause 14 of the Bill is not proportionate to the magnitude of the crimes, and ought to be reconsidered and increased to be a stronger deterrent.

## **HARMONISATION OF LEGISLATIVE FRAMEWORKS AND OBLIGATIONS**

16. We note that Chapter 9 of the Bill prescribes that Electronic Communications Service Providers must intercept and store information as required by State Security agencies. While, our members in principle have no objection to assisting in the lawful gathering of evidence, to enable and contribute to successful prosecutions, they are nevertheless concerned about the conflicts of the different and conflicting legislative provisions by which they are enjoined.

17. Telecommunications or electronic communications networks can be likened to road infrastructure, where the local, provincial or national governments build and own the road network but anyone can use the network. Users are bound by specific rules that ensure fair and safe usage of the network, however, the regulating authority and owners of the infrastructure are unable to access the contents of the vehicles using its infrastructure. Instead, to determine the contents carried across its infrastructure relevant authorities would need to enable a lawful interception.

18. Similarly, telecommunications networks providers do not have access to information carried over its networks, unless intercepted under specific circumstances as a result of strict prescribed legislative processes.

19. The prohibition on telecommunications providers from accessing information and following strict processes to intercept information is to ensure effective consumer protection and privacy. Telecommunications providers are further prohibited from storing any such information.
20. Our members are nevertheless concerned that the Bill, has provisions which contradict the legislative provisions. While, the intentions are a noble attempt to cure specific problems, it places network providers in a precarious position as compliance with one set of legislation will result in non-compliance with another set of legislation. How would a network licensee determine which legislation to comply with and which to disregard? This places our members in an unenviable and reckless position which will undoubtedly compromise good corporate governance.
21. Consequently, we implore the Department to reconsider the current provisions to ensure alignment with legislative provisions to enable telecommunications networks providers to lawfully assist the security agencies.
22. To illustrate the point section 27 of the Bill contradicts the provisions of sections 16 -19 of the Regulations for the Interception of Communications-Related Information Act (RICA). We accordingly, propose that the current provision for evidence gathering in sections 16 -19 of RICA be incorporated into the Bill. We are of the view that this will eliminate contradictory provisions for evidence gathering for entities subject to RICA, while also creating an applicable framework for entities not subject to RICA.

## **INTERGOVERNMENT DEPENDENCIES**

23. The implementation of the Bill has many dependencies which resides across various government departments. We would like to caution the Department, of the considerable risks of the dependencies set out in the Bill. When a deliverable or milestone is dependent on an action the absence or delay of that action has a knock-on effect. Consequently, we

therefore propose that the department reconsider the dependencies included in the Bill to ensure the effective implementation thereof.

### **COSTS OF COMPLIANCE**

24. The improved clarity in respect of standards is welcomed, however, we would like to caution the Department on being too prescriptive in the technical details. Instead, determination of the standards and desired requirements in our view will suffice.

25. While, our members support the Bill and its intentions, they are nevertheless concerned about the costs of compliance. This becomes a critical concern in the communications sector as this is a sector characterised by being required to continually provide services at higher speeds, better quality of service and at lower prices. As a result, it becomes imperative that our members keep a tight rein on input costs.

26. Prescribing the outcome and the standard allows innovation in achieving the objectives.

### **TIMELINES**

27. While, SACF members support the Bill, and acknowledge its need for expedient implementation, it is of the view that much systems development will be required to give effect to the provisions. Therefore, it ought to be done incrementally to make implementation more manageable from cost and implementation perspectives.

28. Accordingly, we propose that implementation must adopt a phased approach and that the timelines are aligned to stakeholder comments.

29. We thank the Department for the opportunity to submit comments on the Bill.