**Cybercrimes and Cybersecurity Bill, South Africa**

1. **Introduction**
   1. We congratulate the South African government on taking cybersecurity seriously and having a considered, thoughtful approach to what legislation could look like.
   2. We take concern about security and safety very seriously, including that relating to child sexual exploitation, bullying and harassment and terrorism.
   3. We are delighted that the government continues to show leadership in this critical area of security and that we have an opportunity to hand in some thoughts on this important matter.
2. **Overview**
   1. Privacy and cybersecurity are very important to us. Finding the right balance between protecting security/privacy and enabling business and innovation can be tough, but it's an important balance to find. We want to ensure the latest technology can be both adopted and developed in South Africa. We want to ensure speech issues are not mixed up with cyber security. We want to be sure that there are not onerous intermediary liabilities on internet companies. We want to be sure that the legislation resolves and does not create conflict of laws or duplication of effort internationally.
   2. We would like to congratulate the South African government on addressing cybercrime and cybersecurity, and including in their strategy:
      1. a co-ordinated national response, including education for individuals and companies and maintaining technical expertise in cybercrime investigators;
      2. following international best practice, whilst acknowledging this is evolving;
      3. an attempt to not over-criminalise acts that may be carried out for legitimate purposes;
   3. We would like to congratulate the South African government on its international and multi-stakeholder approach to this issue:
      1. in consulting internationally;
      2. acknowledging that solutions need the support of an international and multi-stakeholder community, including bilateral agreements with other countries and joint working with the private sector;
   4. We would like to congratulate the South African government on its legal process model, in particular:
      1. clarity on legal processes and powers to investigate, search, access or seize electronic evidence;
      2. the criminalization of wrongful seizing and searching of devices and retention of data;
      3. clarity of legal processes and powers to preservation of data, requests for retention of data and requests for real time traffic data:
   5. We are encouraged by this important piece of legislation, seeking to follow international norms in developing international best practice. This includes creating a national body responsible for cybersecurity policy in South Africa and updating legislation on:
      1. private-public partnership on cyber security;
      2. protecting critical national infrastructure against cyber attack;
      3. digital evidence gathering;
      4. mutual legal assistance and international 24/7 points of contact.
   6. Below we detail some remarks and suggestions about a few chapters, specifically around criminalising malicious communication, concerns around considerations of conflict of laws and responsibility around identifying cybercrime. We detail our concern below in summary and in detail.
3. **Summary Remarks**
   1. The Bill **criminalizes malicious communications** – namely messages that result in harm to person or property, such as revenge porn or cyber bullying.
      1. in international best practice, to avoid criticism of cybercrime legislation being used for censorship, this is usually dealt with separately;
      2. The malicious communications part of the Bill also makes it a **criminal offense for companies not to comply with court orders to remove data** or to supply the details of the individual who posted the information;
   2. The Bill **augments local jurisdiction** where the crime is not only committed in SA, but inter alia, if the effect of it is felt in the country.
      1. Whilst we understand the need to confront the issue of jurisdiction, South Africa should explicitly deal with issues of conflict of laws, duplication of effort and double jeopardy (where an individual could be tried twice, in two different countries, for the same crime.
      2. This is particularly true when the individual is changed with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offense, and the number of jurisdictions could be very wide.
   3. The Bill **mandates a level of responsibility for identifying cybercrime**, storing evidence and reporting;
      1. It imposes onerous obligations on electronic communications service providers, including Facebook, to assist in the investigation of cybercrimes, but also to report them no later than 72 hours. This provision lacks clarity and is likely to create duplication of effort internationally.
      2. It creates something that sits between voluntary and mandatory cross sector information sharing - if a sector does not set up voluntary information sharing, the South African government can mandate it. It can also, if it wishes, regulate the type of information shared, and create a criminal offense of not sharing this information.
   4. The Bill **mandates the** provision of live time traffic data, data whose preservation has been requested and specific fields related to BSI which we may not have.
      1. These all have conflict of law issues.
4. **Details of Submissions**

**Chapter 3: Malicious communications:**

* 1. *Sec 19* allows a judge to serve a removal order on an individual or an internet company. We have a few questions about the intermediary liability responsibility of companies.
     1. We suggest that requests should first be made to the individual to remove the content and/ or explain its sharing. Only if this is not possible should an approach be made to the internet company
     2. Non-compliance with the order appears to be a criminal offense. Despite the fact that this section allows an appeal to the judge, we are concerned that the criminalization of non-compliance by internet companies sets a bad precedent internationally and will undermine good will amongst internet companies to remove content;
  2. *Sec 20* allows a judge to request data from the internet company on the individual who created the malicious content. We would like to indicate that:
     1. much of the data identified is not routinely requested by or stored by internet companies. For example, we do not require a physical address;
     2. provision of this data may be precluded by conflict of laws, dependent on the nationality and location of the person and the exact nature of the offence;
     3. making individual employees personally liable appears disproportionate and may go against international best practice; and
     4. criminalization of non-compliance by internet companies also sets a bad precedent internationally and will undermine good will amongst internet companies to provide this information.

**Chapter 4: Jurisdiction**

* 1. *Sec 23* has a wide-ranging expansion of jurisdiction, in particular with respect to malicious communications.
     1. Whilst we understand the need to confront the issue of jurisdiction with respect to cyberspace, we suggest that this section explicitly deal with issues of:
        1. conflict of laws. This is particularly true when the individual is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offense, and the number of jurisdictions could be very wide.
        2. double jeopardy (where an individual could be tried twice, in two different countries, for the same crime). This is particularly true when the individual is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offense, and the number of jurisdictions could be very wide.

**Chpt 5: Powers to investigate, search, access or seize**

* 1. *Sec 32* makes it mandatory to provide technical (or any other) assistance to law enforcement.
     1. Whilst we understand the need to confront the issue of jurisdiction with respect to cyberspace, we suggest this section explicitly deal with issues of conflict of laws, where provision of such assistance would be breaking the law of the country of incorporation or nationality of the alleged perpetrator;
     2. In addition, criminalization of non-compliance by internet companies may set a bad precedent internationally and will undermine the good will amongst internet companies to provide this support;
  2. *Sec 37* makes it an offence to reveal requests for information that we have provided. We would caution against this, and believe it counters best practice as outlined in our [Reform Government Surveillance principles](https://www.reformgovernmentsurveillance.com/).
  3. *Sec 38* focuses on the provision of real time communication related data, preservations and retention of data.
     1. Whilst we understand the vital need to deal with all of these in investigating cybercrime and cyber-related crime and conflict of laws. We suggest explicit reference is made here to Chapter 6 s49.
     2. criminalization of non-compliance by internet companies sets a bad precedent internationally and will undermine good will amongst internet companies to provide this support.
  4. *Sec 39 (9)* criminalization non-compliance by internet companies on data preservation. This sets a bad precedent internationally and will undermine good will amongst internet companies to provide this support.
  5. *Sec 42 (9)* criminalization of non-compliance by internet companies on data provision. We would like some clarity on the conflict of laws, where provision of such assistance would be breaking the law of the country of incorporation or nationality of the alleged perpetrator, unless Mutual Legal Assistance is used. We suggest explicit reference is made here to Chapter 6 Sec 49.

**Chapter 9:** **Obligations of Electronic Communications Service Providers**

* 1. *Sec 52* requires companies to retain a level of awareness (although not to actively monitor systems), identify and disclose any cybercrime offences with 72 hours to the South African Police Service;
     1. we would be grateful for greater legal clarity on what constitutes becoming 'aware'. For example, many companies experience numerous indications of attacks on systems every day that may or may not constitute cybercrime offences and have no direct relationship to South Africa.
     2. We would also be grateful if this section also acknowledged other existing obligations to report internationally, and sought to reduce duplication of effort by stressing the working together of national Computer Exploitation Response Teams;
  2. *Sec 52 (3)* deals with the criminalization of non-compliance by companies. We would like some clarity on:
     1. onerous duplication of effort; and
     2. the setting a bad precedent internationally that will undermine good will amongst internet companies to provide this support;

1. **Chapter 10: Structures to deal with Cybersecurity**
   1. *Sec 55* mandates the creation of information sharing nodes for different sectors of companies. It also allows for the further regulation of the information shared within the 'node.' There are some concerns about:
      1. the onerous duplication of effort and cost, where other similar systems exist internationally;
      2. the setting of a bad precedent internationally that will undermine good will amongst internet companies to provide this support; and
      3. the emphasis on government regulation, which may create criminal offenses of not sharing specific types of data, where the private sector is best placed to access what information is useful to share with other sectors.
   2. *Sec 56* allows for the regulation of information sharing. We believe that any such regulation should take into account the following, and we suggest that this should explicitly be contained in this provision:
      1. onerous duplication of effort and cost, where other similar systems exist internationally;
      2. the setting of a bad precedent internationally may undermine good will amongst internet companies to provide this support; and
      3. the emphasis on government regulation, which may create criminal offenses of not sharing specific types of data, where the private sector is best placed to access what information is useful to share with other sectors.
2. **Conclusion**
   1. Facebook greatly appreciates the continued opportunity to contribute to discussions on cybersecurity in South Africa.

**FACEBOOK**

**EBELE OKOBI**

**10 AUGUST 2017**