BARASA KIJIRAH
ADVOCATES

Office D4, 2nd Floor, Riara centre, Riara road, Nairobi
P. O. Box 14637 00100, Nairobi
Tel: +254 720 633 821 | +254 724 622 619
Email: info@barasakijirahadvocates.com
Website: www.barasakijirahadvocates.com

PIN: P051650396M

DATA PROTECTION BILL COMMENTS

ABOUT THE AUTHOR MALCOLM KIJIRAH

I am a lawyer and Partner of a Law firm in Nairobi, Barasa and Kijirah Advocates. I have tertiary qualifications in both Information Technology and Law, and have worked at the nexus of both for the majority of my career.

My immediate preceding professional role was overseas in Australia prior to my return to Kenya in 2016 working in Telecommunications and IT Law for the Federal Australian Attorney-General's Department and in particular, I helped develop and implement the Data Retention laws in Australia which this paper concerns.

KEY POINTS

- There is an opportunity to be forward thinking and expound on or begin work on expanding ***the Data Retention*** sections of this bill.
- This is currently prescribed very broadly as a clauses in the Bill in s (6) and s (19) and undoubtedly will eventually create a tension between the national security space and personal privacy of individual's data.
- Eventually from a privacy and National security perspective, Kenya will, like many other jurisdictions require Data Retention legislation and/or regulations specifically for its Telecommunications Industry (for National security purposes). This is therefore a much narrower field in relation to data and privacy but a relevant one for consideration. It is prudent to start considering this now as we develop the legislative environment surrounding this.

COMMENTS

The Bill seeks to give life to Article 31 of the Constitution 2010 which states, "Every person has the right to privacy, which includes the right not to have their person, home or property searched, their possessions seized,

information relating to their family or private affairs unnecessarily required or revealed, or the privacy of their communications infringed."

My comments relates less from the personal privacy perspective, but more from a National security perspective as outlined in clause 6(2)(a) and (b) which outline that the right to privacy may be limited for purposes of :

(a) National security;
(b) Prevention, detection, investigation, prosecution or punishment of a crime;

In developing this Bill there is an opportunity either now or if time does not permit, later through an amendment or additional Act to strengthen the provisions of this bill that overlap or concurrently run with National Security interests relating to data retention and access to this data.

In particular there is room to strengthen s (15) of the Act in relation to the protection and security of personal data as well as s (19) that relates to the retention of Information.

S15 of the Bill will require more detail on the security measures that organizations must take to secure the data they have in relation to citizens. This is from a national security perspective very important particularly for organization in the telecommunications Industry such as carriers, carriage service providers and internet service providers such as Safaricom, Airtel, Orange etc.

WHAT IS DATA RETENTION?

Data Retention will require Kenyan telecommunications companies to retain a particular set of telecommunications data for a set period of time (usually at least two years).

These obligations ensure Kenya's law enforcement and security agencies are lawfully able to access data, subject to strict controls. Access to data is central to almost all serious criminal and national security investigations.

In the context of the data retention obligations, data is information about a communication rather than the content or substance of a communication:

- For phone calls, data includes the phone numbers of the people talking to each other and how long they talked for—not what they said.
- For emails, data is information such as the relevant email addresses and when it was sent—not the subject line of the email or its content.

These data retention obligations generally do not require companies to retain data that may amount to a person's web-browsing history.

Data is used in almost every serious criminal or national security investigation, including murder, counter-terrorism, counter-espionage, sexual assault and kidnapping cases. National Security Agencies use data to:

- quickly rule innocent people out from suspicion and further investigation
- identify suspects and networks of criminal associates
- support applications for warrants to use more complex and intrusive tools, such as interception
- support prosecutions as evidence.

Access to telecommunications data under any proposed data retention scheme will be subject to a number of safeguards. In particular:

- access to data is limited to a defined list of law enforcement and national security agencies
- agencies that may access data are subject to independent oversight body
- the relevant Ministry reports to Parliament on the operation of the data retention scheme each year
- where agencies like NIS or enforcement agencies require access for example to a journalist's data for the purpose of identifying a source, those agencies are required to obtain a warrant, and report all such requests to their respective independent oversight body.

Again I note that this is very relevant to the current bill because data retained by the telecommunications industry under the Act is personal information for the purposes of the Data Protection Bill (when assented to).

CONCLUSION

The above comments are to provide insight to the Ministry on a more future facing Data Protection Act (or associated Act) that will have further and more detailed national security considerations particularly given the current terrorism, cybercrime and other security risks we face.

Eventually, as currently drafted, there will be a tension between personal privacy rights and national security requirements. More transparency will eventually be demanded by the public and currently the Bill does not adequately cater to the information that National Security agencies require, how they use it and what oversight there is in this regard. I am proposing the need for a more detailed legislative regime to accompany this sub-section of the bill.

This will require further review and drafting of legislation specifically catering to data retention in the National security space.

I am willing to provide more detailed information on the development of a data retention regime in Kenya should the need arise (and it will most certainly in the near future). My contact details can be found below.

CONTACTS OF THE AUTHOR

Malcolm Kijirah
Senior Partner
Barasa & Kijirah Advocates
Tel: 0724622619
Email: mkijirah@barasakijirahadvocates.com