WHAT KENYAN GOVERNMENT CAN DO TO PREVENT MISUSE OF PERSONNEL DATA BY AGENCY

The right to move data

Part of the reason why breaches cause so much damage is because data is concentrated in the hands of a few providers and dominance of a few key players. The bottom line of all this is the way digital companies have evolved, it's all based on data. The more data you have, the more advertising revenue. The risk is that when there's so much data held by these companies it can easily be misused or misrepresented.

New legislation could be the means to break up this dominant pattern. There should be a software or a mechanism whereby Kenyan citizens are given the right to request that any data held on them by companies be deleted shared with another provider. Citizens should have the power to move their data from one provider to another, creating the opportunity for new business models to emerge.

What are the distinctive protections of the proposed mechanism?

In most circumstances, companies, governments, and other organizations must now obtain genuine and informed consent before they can collect, use, or share a person's personal data. The request for consent must be clearly distinguishable, in an intelligible and easily accessible form, and use clear and plain language. In other words, the request for consent has to be easy to find, and easy to understand.

Special protections should apply to sensitive information.

Processing certain special categories of sensitive data should be very tightly regulated. These include information revealing someone's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as data about genetics, health, and biometrics for example, fingerprints, facial recognition and other body measurements.

What should happen if companies and other institutions don't comply with the Data protection Bill 2018?

The Government regulation should impose stiff penalties on public and private sector organizations that violate its terms. For example, regulators can fine companies up to 5 million Kenya Shillings or 10 percent of annual global turnover (revenue) for non-compliance, whichever is larger.

What effect will the proposed Mechanism have outside Kenya

THE DATA PROTECTION BILL, 2018 is likely to become a global standard because it will apply to any organization that collects or processes the data of Kenyan citizens, regardless of where the organization is based or where the data is processed. It is also possible that other

African countries will copy some or many of its protections as they modernize or establish data protection laws.

The mechanism may become the standard many organizations follow by default everywhere, or at least elements of it. Some multinational companies may choose to apply the regulation to everyone worldwide, while others may attempt to identify and apply a separate set of rules for people in the Kenya. Still other businesses may exit Kenyan market altogether or temporarily block people in the Kenyan while they work to come into compliance. In other cases, systems developed in response to the regulation, like data portability, could be easily offered for users outside Kenya once they are in place.

What impact should the bill have on freedom of expression?

The regulations should provide for a right to erasure. This provision expands what has become known as the "right to be forgotten Under the new "mechanism" individuals can ask companies to erase personal data in specific circumstances: for example, if the data is no longer necessary for the purposes for which it was collected; if the individual withdraws consent or objects and there is no overriding justification for keeping it; or if the data was otherwise unlawfully processed in breach of the 2018 BILL of Data protection. This right also applies if the personal data has been made public, raising considerable implementation difficulties given the ease with which online information can be copied and shared across multiple websites in various jurisdictions.

What else needs to be done to protect data and the right to privacy?

The 2018 data protection bill is a vital step toward stronger privacy protections. However, it will not be effective without interpretation, implementation, and enforcement.

National data protection authorities will need to rigorously respond to complaints, promptly investigate breaches, and actively pursue investigations to enforce the provisions. Many data protection authorities are poorly resourced, and under staffed particularly in comparison to large companies, and lack the capacity to play a comprehensive enforcement role. Member states should allocate appropriate financial and human resources to data protection authorities.

Even with strong enforcement, there are still many structural challenges to achieving the Kenyan ICT ministry vision of data privacy and control. For one, while the regulation requires consent before companies can collect or process data, meaningful informed consent is difficult to achieve without choice. Many large online services have few real competitors, so users are faced with either consenting to a social network's terms or missing out on a central component of modern social or professional life.

In addition, informed consent will only become more elusive over time as advertising ecosystems become more complex. The Bill regulation doesn't directly challenge ad-driven business models that invite users to trade their personal data for free online services like email, social networking, or search engines – all while using that data to create detailed profiles to sell to advertising networks. The average user may consent to data processing without a true

understanding of the complexities of how their data will be used, despite the regulation's requirement of clear privacy notices. Ultimately, the digital society may require many more substantive protections than a consent-based model can provide.

Compiled by: Abraham M Kilonzo

Professional: ICT personnel

Contact: 0727485834