facebook

By Electronic Mail October 2, 2018

Mr. Jerome Ochieng
Principal Secretary, ICT & Innovation
Ministry of Information Technology and Communication
Teleposta Towers
P.O. Box 30025-00100
NAIROBI
pdp@information.go.ke; pdp@ca.go.ke

Chairperson
Taskforce on Development of the Policy and Regulatory Framework for Privacy and Data Protection in Kenya
Communication Authority of Kenya
P.O. Box 14448

Re: Facebook's Comments re: Policy and Regulatory Framework for Privacy and Data Protection in Kenya, 2018

Dear Mr. Ochieng:

Facebook appreciates the opportunity to provide comments in response to the revised draft of Kenya's Data Protection Act of 2018 (the "Bill" or the "Act") and the accompanying Privacy and Data Protection Policy (the "Policy"). We are pleased to see the tremendous progress that Kenya's data economy has seen in recent years, and hope that our comments will assist the Ministry in continuing this positive trend. In addition, we believe that everyone deserves protections for personal data, and we welcome the Ministry's attention to this important goal.

Kenya's technology infrastructure has advanced at a phenomenal rate, having become 14th in the world for fast mobile internet speeds.[1] In addition, the country's 2013 National Broadband Strategy has helped the country continually outpace its peers in Sub-Saharan Africa for average internet connection speeds more generally.[2] With such tremendous progress in its ICT sector, it is no surprise that Kenya is considered to be at the forefront of technological innovation in Africa.[3]

---

[1] Lily Kuo, *Kenya's mobile internet beats the United States for speed*, Yahoo! Finance (June 8, 2017), https://ca.finance.yahoo.com/news/kenya-mobile-internet-beats-united-153705400.html.

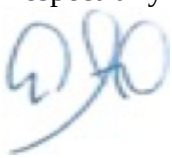
[2] *Id.*

[3] *See, e.g.*, Bitange Ndemo, *How Kenya Became the Cradle of Africa's Technological Innovation*, Newsweek (Dec. 27, 2016), https://www.newsweek.com/how-kenya-became-cradle-africas-ict-innovation-534694.

With that in mind, we are encouraged by the fact that the draft Bill and Policy reflect several valuable privacy practices that should govern Kenya's data economy. Namely, the Bill and Policy take a technology-neutral approach to providing people with consistent expectations about how their data will be handled, and consistent expectations about how they will be informed about their privacy. At Facebook, we believe that transparency and user control are of utmost importance, and the Task Force clearly had those same values in mind when drafting the proposed Bill and Policy. In addition, the Bill and Policy adopt many positive provisions similar to those found in international data protection laws (such as the General Data Protection Regulation ("GDPR")), while, at the same time, avoiding some of the mistakes that other countries have made in regulating the ICT sector.

In the spirit of providing privacy protections that empower individuals and are implementable by innovators, we wish to highlight some aspects of the Bill and Policy that may need further consideration in light of Kenya's goals for its digital economy. The comments below represent Facebook's recommendations for improving the Bill and Policy by adequately balancing privacy values with other considerations—such as innovation, free expression, and security. We thank you for the opportunity to submit this feedback and would welcome the opportunity to discuss with you these and other issues going forward.

Respectfully submitted,



Ebele Okobi
Public Policy Director, Africa
Facebook, Inc.

facebook

1. Registration Requirements for Data Controllers and Processors

Under the draft Bill, no person is permitted to act as a data controller or data processor unless they officially register with the Data Commissioner. Registration requires, among other things, various disclosures regarding the applicant's planned data processing activities, as well as a general description of risks and the security mechanisms put in place to mitigate such risks. In addition, any changes related to prior disclosures must be notified to the Data Commissioner, and registration certificates must be renewed every three years.

Although we are encouraged that the revised draft of the Bill no longer contemplates requiring the payment of fees upon registration, we nevertheless believe that this provision will impose a significant burden on technology innovators—particularly startups that may not have each element of the required disclosures completely figured out at the time of registration. Moreover, an important part of maintaining a robust data infrastructure is making rapid changes in response to emerging security challenges or other changed circumstances, and more broadly to provide users with the best possible service. We therefore recommend that the Bill adopt a model that is similar to the GDPR and many other privacy regulatory frameworks globally, which is based not on registration with the government but rather on accountability based on the context of an entity's relationship with a consumer rather. Under this model, companies' obligations with respect to their users' data vary in-time with their practices—which will prove to be critical to protecting users' privacy rights in the fast-paced ICT sector.

2. Applicability and Scope

We support and appreciate the goal of providing certainty around the jurisdictional scope of the Bill, including applying the Act to controllers and processors who are both established and process data within Kenya. We believe, however, that the scope of the Bill could be clarified further by making its definitions more precise and in-line with foreign data protection laws. For example:

- ***Personal Data***: The definition of "personal data" is quite broad, as it applies to all "natural persons." As explained above, we recommend appropriately limiting the Bill's applicability by clarifying that "personal data" belongs to data subjects *in Kenya*. This would help avoid conflicts with other countries' laws, which might apply different protections for the data of their residents. We also suggest revising the definition to account for information that is linked may be "reasonably linked" to data subjects, rather than information that is merely "relating to" a specific natural person. For instance, "a person has brown hair" arguably "relat[es] to" a natural person, but, without more, it could not be linked back to that person. In addition, we suggest aligning the definition with international standards by specifying that information that has been de-identified or that is obtainable from publicly available sources is excluded from the definition.

- ***Sensitive Personal Data***: We recognize and agree with the importance of protecting personal data that is especially sensitive. However, we believe the current definition of "sensitive personal data" should be narrowed to more clearly identify the data that requires enhanced protection. For instance, information such as an individual's "belief," and "personal preferences" are typically not considered to be "sensitive" by international data privacy standards, and this language could be read, for example, to encompass almost any statement of opinion by an individual. Likewise, "location" data should be narrowed to cover precise GPS locations – not location in general, which could include the country where a person is located or more general types of location that are reflected in the Internet protocol address a person uses on a network.

- ***Third Party***: Given the restrictions that apply to the transfer of data to third parties, we recommend excluding from this definition entities or individuals to whom data subjects direct disclosure – that is, if a person intentionally posts information on Facebook and shares it with a group of people, for example, those people should not be considered "third parties" for the purpose of Facebook's disclosure of the information to those people. Likewise, other exclusions from the definition of "third party" may be appropriate, such as when an organization shares information with its service provider for a particular lawful purpose.

3. Lawful Processing of Personal Data and Sensitive Personal Data

We commend the Ministry for moving away from its previous approach that relied heavily on consent in favor of the model provided by Article 6 of the GDPR, which recognizes multiple legal bases under which data may be processed (including consent). This model acknowledges that consent is an essential legal basis, but it may not always be appropriate in every circumstance. In fact, research shows that requiring consent too frequently can result in what is known as "consent fatigue," in which users are asked to provide consent so frequently that they stop paying attention to the privacy notices presented to them.

Consistent with these improvements, we encourage the Ministry to amend the bill to focus more directly on people's expectations about how their information will be used – imposing higher obligations in cases where a use is inconsistent with the context in which information was collected or the entity's relationship with the data subject. This standard appropriately protects user privacy while focusing on prominent consent or notice interactions in the cases where data use would not be expected. In addition, with respect to sensitive data, we recommend against prescribing specific entities that may process sensitive information and the specific purposes for which the information may be processed. Instead, and particularly in view of the breadth of the "sensitive" concept discussed above, we believe it is important that people have the ability to choose to allow their information – including information they may be considered sensitive – to be used in certain ways. We recommend enabling people to consent to the uses of the information, including sensitive personal data, that they consider appropriate.

4. Data Processing Obligations and Restrictions

The Bill provides several collection, purpose, and retention restrictions that are incompatible with the flexibility required for a modern data economy. As an overarching principle, we support the Bill's notion that data should be processed "lawfully, fairly, and in a transparent manner." However, the Bill also requires that personal data only be collected for "explicit, specified, and legitimate" purposes," "not further processed in a manner incompatible with those purposes," and that all personal data collected be "adequate, relevant, and limited to what is *necessary* in relation to the purposes for which it is processed." In addition, the Bill requires that collected personal data be "kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data" be erased or rectified without delay.

Although we believe that it is important for people to know when their information will be used for purposes that are significantly different from what they were originally told, the Bill should reflect that data may reasonably be collected for more than one purpose in the first instance, and that some differences in processing are minor and may not raise significant privacy concerns. Indeed, the reasonable data subject has certain expectations that his or her information may be used and processed in a variety of ways in order to offer a variety of services.

We also are concerned that restricting data use to uses that are "necessary" for a given purpose may be overly restrictive. In many instances, it may be possible to provide an inferior product or perform a task less well with less data – that is, the additional data processing may not be "necessary" – but people may prefer to have a more personalized experience or other improved services through the use of additional data. To address this concern, we encourage the Ministry to consider the concept of "compatible" purposes reflected in the GDPR. For example, the Bill could allow data to be used for additional purposes as long as those purposes are not incompatible with purpose disclosures that were provided to the data subject.

Finally, we suggest removing the requirement that data be kept "up to date." First, we anticipate that this requirement will be too burdensome for many organizations, especially when the data subject is in the best position to identify and correct inaccuracies in their own personal data. In Facebook's context, we are also concerned that a requirement to keep information about people up to date would create privacy challenges. For instance, if Person A posts about Person B, we would suggest that it would be unexpected for Facebook to have an obligation to continually assess the accuracy or currency of Person A's post.

The Bill also requires that personal data be obtained directly from the data subject unless certain enumerated exceptions apply. However, there are many cases in which it would be appropriate to collect information *about* an individual (but not *from* that individual). For example, it is common for people to communicate privately to or about others, or to share posts or photographs that include others. It is also common for businesses to address communications to people they want to reach – for example, sending a letter or electronic message to a particular recipient, which has the effect of communicating the recipient's identity to the organization that delivers the message. While this obligation may not be intended to prohibit these types of communications, we encourage the Ministry to remove or narrow this provision so that it enables these types of communications.

5. Cross-Border Transfers and Data Localization Requirements

We believe that data protection legislation should encourage, rather than hinder, the global interoperability of technologies. Limits to cross-border data flows, such as those contained in the draft Bill, present serous challenges to data prosperity and innovation without significantly enhancing data security or privacy. Indeed, McKinsey estimates that cross border data flows have added more than 10% to world GDP, and the European Centre for International Political Economy estimates that economy-wide data localization requirements could lead to domestic GDP losses of as much as 1%.[4] And research conducted by the OECD, the World Bank, and Facebook suggests that small and medium-sized businesses that engage in global trade are five percent more confident in their businesses and ten percent more likely to have added local jobs in the preceding six months than non-traders.[5] In short, promoting cross-border communication is a critical component of preserving and promoting economic growth.

As such, rather than applying strict conditions on data transfers, we suggest requiring that organizations, under their respective legal regimes, remain accountable for the continued protection of transferred data. If controllers of data remain accountable for its use and transfer, prohibitions on onward-transfer of data outside of the country of origin are unnecessary. This approach would preserve protections for data subject to the Bill, without imposing limitations that could constrain Kenyan businesses from growing globally.

Moreover, we recommend removing the requirement that every data controller and processor ensure that at least one serving copy of personal data be stored on a server or data center in Kenya. This requirement would create a meaningful disincentive for foreign companies that may otherwise wish to establish a presence in Kenya's data economy, both because of the raw costs of creating duplicative storage of data and the logistical difficulties in segregating data covered by the Bill from data that is not covered. These burdens also would be felt disproportionately by small and medium-sized businesses, which lack the resources of larger companies to pay the costs of duplicative infrastructure. Likewise, localization obligations could discourage businesses located outside Kenya to partner with Kenyan businesses for data processing, if doing so would require the Kenyan processor to make a copy of any data to which it has access or increase the cost of doing business with a Kenyan processor as compared to a processor located in a country without a localization requirement.

We also do not believe that a localization requirement is necessary to promote the privacy of Kenyans, and could, in fact, undermine privacy by requiring additional copies of data that could theoretically become subject to unauthorized access. Nor is this requirement needed to

---

[4] European Centre for International Political Economy, "The Costs of Data Localisation: Friendly Fire on Economic Recovery," http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf (2014).

[5] OECD, World Bank & Facebook, Future of Business Survey: Trade Report, https://eu.futureofbusinesssurvey.org/manager/Storyboard/fileHandler.ashx?file=170726%20Future%20of%20Business%20Survey%20-%20Trade%20report%20July%202017.pdf (Aug. 2017).

ensure adequate protection of personal information under the Bill. Indeed, the existing draft covers processing of data by organizations established in Kenya even when that processing occurs elsewhere.

For these reasons, we believe that the existing obligations reflected in the Bill are sufficient to protect Kenyans' privacy, without the disadvantages that localization mandates and data transfer restrictions would create.

6. Data Subject Rights

We believe that everyone deserves strong privacy protections, including many of the data subject rights reflected in the Bill, and we support the idea that people should have basic protections for their data across organizations. As the Ministry considers the specific approach to adopting these data subject rights, we encourage you to anticipate situations where those rights should be limited to protect other important interests, and clarify that data subject rights would not apply in situations where exercising these rights would: (1) enable fraud or other unlawful activity, (2) interfere with law enforcement or judicial activity, (3) undermine privacy or data security interests of others, (4) be unduly burdensome or excessive, (4) reveal proprietary assets or business insights, or (5) require the collection or processing of additional personal information about the consumer.

These clarifications are important, for example, to ensure that an attacker cannot take advantage of data subject rights to modify records of his or her efforts to undermine information security, which records could lead to his or her detection. They also ensure that one person cannot invade the privacy of another person's private electronic mail messages, for example, simply because the first person is mentioned in an e-mail.

We also encourage the Ministry to recognize that the exercise of certain data subject rights may mean that an organization will not provide requested products or services to an individual. For instance, if a particular service relies on the processing of a particular piece of data, the organization providing that service may not be able to provide the service if the data subject does not allow the data processing. For similar reasons, when a person exercises the right to object to the use of his or her information for direct marketing, the Bill should anticipate that a company may no longer provide services that are funded through advertising to a person who does not wish to see ads. To avoid these unanticipated complications, the Ministry might decide to amend the right to object to processing of data so that it extends only to uses of data that are materially inconsistent with the uses disclosed by the data controller/processor, or with the relationship between the data subject and the data controller/processor.

Finally, we recommend that the notice obligations under the Bill be modified so that notice is not required to be given *before* the collection of personal data. Although prior notice is in many cases desirable, research suggests that in many instances just-in-time notice – that is, notice contemporaneous with the data collection – is preferable, and may in some instances be a more effective way to educate people about their information data. For instance, when people share photographs on Facebook, they are given the opportunity to review and control whom they are sharing such photographs with at the same time. We believe that this type of just-in time privacy notification can be effective at informing users of their choices than lengthy privacy

notices presented to them when they first start using our service, and we encourage the Ministry to revise the Bill's notification requirements to accommodate the other creative ways in which other organizations may provide privacy information to people.

7. Protecting Children

The revised Bill introduces several new restrictions and requirements with respect to processing children's personal data. For example, the Bill requires that data controllers and processors wishing to process children's personal data implement "appropriate mechanisms" for both age verification as well as parental consent. Such requirements are similar to efforts made in the United States and elsewhere to enable children to explore the internet safely, and it therefore may be helpful to consider some of the challenges those efforts have faced as Kenya's Bill moves forward.

With respect to parental consent and age verification, we are encouraged by the fact that the Bill does not prescribe specific methods of obtaining such consent, recognizing that the specific methods may vary depending on the organization's relationship with the parent. In the United States, for example, one permitted method for validating parental consent is requiring parents to submit their credit card numbers (which a child presumably would not have access to), but this mechanism may not work in regions in which payment cards are not as prevalent. Some companies have opted to require parents to print, sign, and fax a consent form, but this method tends to be too slow and cumbersome. Given the breadth of Kenya's mobile internet economy, mechanisms that require parents to text their consent may be a viable option.

We are concerned, however, that language in the Bill around age verification goes beyond standards applied in other jurisdictions, such as the GDPR in Europe and the Children's Online Privacy Protection Act (COPPA) in the United States, and should follow the majority of other jurisdictions imposing child-protection measures by clearly applying any restrictions on children's data to children under 13. Broader requirements – including an obligations to verify the age of a child – could unintentionally undermine privacy by requiring organizations to collect and verify the identities of anyone using their services (and thereby require the collection of substantially more personal information), in order to determine whether or not the person is misrepresenting his or her age. Providing clearer guidance that protections of children's data apply to children under 13 and avoiding any suggestion that additional privacy-invasive measures are needed for the purpose of age verification would help avoid these unintended outcomes.

8. Data Security and Breach Notification

The Bill contains many sensible data security requirements and improves on the data notification requirements of other countries in several meaningful ways. Notably, the breach notification obligations provide data controllers with sufficient time to investigate data security incidents before satisfying reporting requirements, addressing concerns from regulators in some other jurisdictions who may get incident reports before the specifics of an incident are known. We recommend that the Bill retain this approach, rather than prescribing, at a later date, a

specific timeframe during which notification must occur.

In addition, we recommend narrowing the breach notification obligations to circumstances in which the breach is likely to result in a material risk to the rights and freedoms of natural persons. With this limitation, which is similar to that adopted in other breach notification legislation, the Data Commissioner's resources can be directed to significant data security incidents, rather than addressing individual situations where, for example, a customer service representative inadvertently views a data subject's information but rectifies the situation immediately.

9. Governance and Enforcement

The text establishes the Office of the Data Protection Commissioner to enforce the Act—an approach that we support given the importance of having a single regulator empowered to interpret and enforce the Act's provisions. We are also encouraged by the fact that the Commissioner is explicitly charged with promoting self-regulation among controllers and processors and suggest that the Bill also charge the Commissioner with promoting innovation, as well. However, we recommend striking the provision that enables the Data Commissioner to "carry out periodical audits of the systems held by data controllers or processors." Provisions enabling government access to people's private data – even for the purpose of providing privacy protections – are unusual and typically subject to high burdens involving a court order and an ongoing investigation against the data subject. Adopting provisions that enable unusually broad government access to data raise meaningful concerns for companies that may seek to do business in Kenya, and could also complicate Kenya's effort to achieve findings of adequacy under foreign data protection regimes.

In addition, in several places the Bill contemplates imprisonment as a penalty, an approach that is highly unusual in data protection legislation. To maintain parity with most modern data protection regimes and avoid disincentives for foreign entities to partner with Kenyan businesses or further invest in Kenya, we encourage the Ministry to modify the Bill to focus on financial penalties subject to a reasonable cap, such as a flat amount specified by statute or a percentage of the revenue the entity earned in Kenya during the preceding year.

Finally, we encourage the Ministry to identify opportunities to streamline the language of the Bill – for example, in places where similar obligations are referred to in multiple parts of the Bill – to ensure that organizations will have clear guidance about what is expected of them. In our experience, using different wording in different parts of legislation, or between legislation and a Policy, can make it difficult to understand exactly how to comply with the law. We therefore recommend that definitions and substantive obligations be articulated once within the Bill, and that the Policy be reserved for establishing the purpose of the Bill and explaining the principles underlying its provisions.

* * *

We appreciate the opportunity to provide comments on the draft Bill and look forward to working with the Ministry in its effort to build meaningful data protections for people in Kenya.