Comments by the United States to Kenya's Ministry of Information, Communications and Technology on its Draft Data Protection Bill, 2018

The United States thanks Kenya for the opportunity to comment on the draft Data Protection Bill (hereafter the "draft bill") released in August 2018. Kenya and the United States share an interest in robust privacy protection. This draft bill supports that interest in many ways. However, some aspects of the draft bill appear to depart from long-standing principles that sustain global economic growth and ensure effective regulatory cooperation across borders.

These comments address the provisions of the draft bill that appear to support privacy and economic prosperity, as well as those that could negatively impact both interests. The United States would welcome further dialogue with Kenya on the draft bill and the Privacy and Data Protection Policy (hereafter the "draft policy").

Specific Issues

Part I: Preliminary

Section 2. *Interpretation*

The draft bill defines "anonymisation" as "the irreversible removal of personal identifiers from personal data so that the data subject is no longer identifiable." However, it is not technically feasible to anonymize data irreversibly. A more standard practice seen in the OECD Privacy Guidelines, APEC Privacy Framework, and enacted privacy laws is to support anonymization where it would take extraordinary effort to identify an individual. We recommend a revision to stipulate that data be anonymized so that it cannot be identified "except through extraordinary effort." Aligning the definition of anonymization in the draft bill with international norms or with the definition used by international standard-setting bodies (e.g., the International Organization for Standardization) would help Kenya meet its policy objective of protecting personal data while avoiding placing an undue burden on data processors.

The draft bill seems to extend the reach of Kenyan law in a way that would create regulatory uncertainty for data-intensive businesses with global operations. The definition of "cross-border processing" in the draft bill includes "processing of personal data while outside Kenya but which substantially affects or is likely to substantially affect the data subject in Kenya." Such a broad and vague definition is unprecedented and an extreme departure from international norms. We urge Kenya to exclude from the law's coverage processing of personal data outside of Kenya. However, if Kenya decides to include it, we urge Kenya to limit the definition to processing abroad of the personal data of individuals in Kenya and such processing only in limited circumstances that are clearly spelled out so as to make clear the authority on which Kenya's rests its claim to be able to assert extra-territorial jurisdiction (such as processing the data of individuals in Kenya for the purpose of engaging in business with them). The vague definition in the draft bill will make it difficult – if not impossible in some cases – for companies to determine whether their processing is subject to Kenya's privacy law. Many businesses outside of Kenya, including small- and medium-sized enterprises, that do not target the Kenya market would have no reason to suspect that Kenya's privacy law may apply to their data processing. At the very

least, the definition should be narrowed and clarified so that the law can be followed and enforced appropriately.

For this reason, the United States favors interoperability facilitated by international arrangements like the APEC Cross-Border Privacy Rules System, which offers grounds for clear, predictable means of protecting privacy while facilitating data transfers across borders. In addition, Kenyan firms are free to build additional data protection and privacy requirements into their contracts. Finally, Kenyan enforcement authorities can work through forums like the Global Privacy Enforcement Network to share information about potential privacy harms with authorities in the relevant jurisdictions. Narrowing the application of the law to processing of personal data of individuals in Kenya that occurs within Kenya would reduce the risks of setting a precedent that would be harmful to all countries that hope to benefit from the growth of the global digital economy.

General Comment on Definitions: The draft legislation contains numerous vague or expansive definitions which may present unintended challenges for compliance or overly restrictive uses of non-sensitive data categories. There are common definitions outlined in privacy principles based on the OECD Privacy Guidelines and APEC Privacy Framework which may be usefully incorporated.

For example, "biometrics" is defined as a technique of personal identification based on "physical, physiological, and behavioral characterization." Blood typing is does not permit identification of a unique individual (although it may exclude someone as a suspect because his or her blood type is different). Moreover, the inclusion of the terms "beliefs" and "personal preferences" in the definition of "Sensitive Personal Data" renders the scope of this provision extremely uncertain and subjective. We recommend the addition of the term "religious beliefs" instead. In addition, "of the data subject" at the end of the sentence is confusing, since all the sensitive information pertains to "the natural person" referenced at the beginning of the sentence.

We encourage revisions to these and other definitions through consultation with industry to limit unintended compliance challenges.

Part II: Office of Data Protection Commissioner

Section 8. Powers of the Data Commissioner

The Data Commissioner should have explicit powers to allow international cooperation. Because current privacy and data protection issues increasingly cross borders, enforcement and data flows are facilitated by international cooperation. Section 8(2) can have an additional subsection specifying these powers:

> "Cooperate internationally, including by sharing information with and providing assistance to, foreign authorities enforcing laws that provide protections substantially similar to those provided by the laws enforced by the Authority."

This will clarify that the Commissioner can effectively cooperate internationally to safeguard privacy in Kenya.

Part III: Registration of Data Controllers and Data Processors

Section 15. *Registration of Data Controllers and Data Processors*

Under the draft bill, all data controllers and data processors must register with the Data Commissioner, with some exceptions. A similar registration framework constituted part of the E.U. Privacy Directive, in force between 1995 and 2018, but was dropped after the concept proved unworkable. Such a comprehensive requirement for registration also could prove burdensome for all parties involved; it could discourage small- and medium-sized enterprises, in particular, from engaging in the digital economy in Kenya.

Part IV: Principles and Obligations of Personal Data Protection

Section 22. *Principles of Data Protection*

Section 22(1)(h) requires that any transfers outside of Kenya show adequate proof of the recipient country's adequacy. Without further description, it is unclear how Kenya would perform its adequacy determination and, depending on how adequacy is interpreted, there may be an impediment to data controllers and processors from competing in the digital economy. We recommend the bill make clear that there are many alternative private frameworks that may provide adequate safeguards, such as the self-regulatory frameworks mentioned above, and further discussed below in Section 45.

Section 26. *Duty to Notify*

Section 26(1)(e) requires data controllers or data processors to inform data subjects about their data's intended recipients prior to collecting personal data. The draft bill duly recognizes the potential complexities of such notice in requiring it "as practicable." Nevertheless, if rigidly implemented, this requirement may limit the ability of firms to alter business relationships or contract with new data processors, as updating privacy policies impacts global operations and can be challenging for small and large firms alike. We recommend altering this notice obligation to a more commonly used international approach, by which data fiduciaries must inform data principals of "categories" of individuals or entities with whom data may be shared.

Section 27. *Lawful Processing of Personal Data*

Effective and comprehensive privacy laws allow for a range of grounds for processing, such as legitimate interest, for functions of the state, compliance with law or court orders, employment purposes, and other commonplace grounds for processing data. The inclusion of many of these grounds for data processing in Section 27(1) is a welcome addition to this trend.

Section 34. *Right to Data Portability*

Section 34(1) establishes data subjects' right to data portability such that they have "the right to receive personal data concerning them, which the data subject has provided to a data controller or data processor, in a structured, commonly used and machine-readable format." Data portability is onerous and expensive for certain firms, but many firms are already seeking to provide this service to their customers in response to consumer demand. We encourage Kenya to refine this section in consultation with the private sector – both to adhere to what is technically feasible and to ensure an appropriate scope of data that may be subject to portability requests. Stating a specific timeline for responding to requests for data portability may not adequately provide for the realities of the situation. Instead, requiring response as soon as practicable could both encourage firms to respond more quickly if possible and allow flexibility for more time-intensive requests.

Section 36. *Right of Rectification and Erasure*

Section 36(1)(b) provides for the right of the data subject to request erasure or destruction of personal data that "the data controller or data processor is no longer authorised to retain, [sic] irrelevant, excessive or obtained unlawfully." The draft policy, in Section 6.1.9., characterizes it as a "right to be forgotten/the right to erasure."

A right to be forgotten raises serious concerns regarding freedom of expression and is inconsistent with the open, decentralized nature of the Internet. The United States generally agrees that individuals should be able to withdraw their consent to data processing, within reasonable limits. However, establishing a right to be forgotten presents serious risks of allowing private persons or state authorities to censor expression online. Publicly available information is often replicated across the Internet, making the proposed notification requirement difficult or infeasible to implement. In addition, the draft bill may interfere with U.S. regulatory record preservation requirements, preservation requirements under other U.S. laws or court orders, or lead to the spoliation of evidence necessary in civil litigation or criminal prosecutions.

Part V: Grounds for Processing of Sensitive Personal Data

Section 43. *Further Categories of Sensitive Personal Data*

Section 43(1) authorizes the Data Commissioner to create additional categories for sensitive personal data beyond those defined in Section 2. This approach recognizes that, as technology and society evolve, revising earlier data protection practices may become necessary. But, if implemented without accounting for stakeholders' various equities, there could be unintended consequences for Kenyan businesses and their foreign peers. It would benefit all parties involved to define an approach that balances flexibility and clarity.

Part VI: Transfer of Personal Data Outside Kenya

Section 44. *Rule as to Data Centres and Servers*

Section 44(1) requires "the storage, on a server or data centre located in Kenya, of at least one serving copy of personal data to which this Act applies." This measure would raise costs for firms, especially foreign firms, which are more likely to depend upon data centers located outside Kenya. Mandating local storage also blunts the effectiveness of certain cybersecurity best practices, which themselves play an important role in data protection. One such technique splits an individual's personal information and distributes these segments across multiple servers and regions. A key benefit of this approach is that a hypothetical breach in any one country would expose only a limited subset of data, which may be useless absent the other portions. Though the draft bill would not prevent companies from engaging in such a practice, requiring that a complete set of data be stored in a single country largely undercuts the range of privacy enhancements that distributed systems can bring. Given recent data breaches in markets around the world, it is imperative that regulators not limit the effectiveness of best-in-class protections for data. We urge Kenya to eliminate this data localization requirement that will hinder trade and thwart the draft bill's goal of strengthening protection of personal data.

Section 44(3) prohibits cross-border processing of sensitive personal data. An extensive body of research underscores the economic harms arising from data localization. While we recognize the importance of imposing stringent security measures around, for example, national security data, we are concerned that this set of "sensitive personal data" may be defined in a broader way that would hamper the ability of firms to do business across borders, limit law enforcement and national security cooperation between governments, or result in conflicts of laws for data fiduciaries and processors. We urge Kenya to eliminate this data localization requirement.

The uncertainty arising from the Data Commissioner's ability to create new categories of sensitive personal data amplifies this concern. Moreover, per Section 44(2), the Cabinet Secretary can designate categories of critical personal data that can only be processed in Kenya on grounds of "strategic interests of the state or on protection of revenue." Such a broad and ambiguous authority raises strong concerns for businesses that need a predictable business environment. We strongly encourage Kenya to eliminate this requirement or, at the very least, to provide clarifications about the "protection of revenue" provision, to alleviate uncertainty for businesses operating in Kenya.

Section 45. *Conditions for Transfer out of Kenya*

The grounds for cross-border data transfer outlined in Section 45(1) range in the degree that they would burden the parties involved. Section 45(1)(a) creates a challenge for industry and regulators, as proving "appropriate safeguards" on a case by case basis is burdensome and legally challenging. Lacking a clear definition for "appropriate safeguards," this approach risks slowing the advancement of the digital economy, without guaranteeing substantial gains for privacy. It also limits companies' use of contractual obligations or internal processes which ensure appropriate levels of protection on data transferred out of Kenya. We encourage Kenya to recognize as an appropriate safeguard certifications and codes of conduct for companies – such

as the CBPR certification – which offer enforceable mechanisms for companies to demonstrate compliance with privacy laws. This approach would ensure companies protect data subjects' rights throughout the lifecycle of the data when exported from Kenya without disrupting Kenya's growing digital economy.

In place of the explicit consent outlined in Section 45(1)(b), we support the approach taken in Section 45(1)(c), which recognizes several exceptions to cross-border transfer restrictions that also appear in comparable privacy laws around the world, including: in service of the performance of a contract, public interest, legal claims, data subjects' vital interests, and the legitimate interests of data controllers or data processors. With respect to the "public interest" exception, we recommend that the text specify that the exception would apply to transfers required under laws outside of Kenya. As an example, this would enable transfers to U.S. regulators and other agencies from Kenyan companies subject to U.S. law for their U.S. operations or activities (e.g., in the financial sector). In addition, with respect to the "legal claims" exception, we recommend that it clearly apply to data transfers necessary to investigate, pursue, or defend against legal claims, or when subject to legal process, court rules or court orders outside of Kenya.

Section 46. *Safeguards Prior to Cross Border Transfer*

Section 46(1) empowers the Data Commissioner to require entities transferring data across borders to demonstrate the "effectiveness" of the security safeguards in place. Demonstrating actual effectiveness of safeguards may prove difficult and appears to go beyond the requirements of Section 37(2)(b), which mandates that entities "take reasonable measures" to "establish and maintain appropriate safeguards." Accordingly, we propose changing the text to read:

> "The Data Commissioner may request a person who transfers data to another country to demonstrate the **existence of appropriate security safeguards** or the existence of compelling legitimate interests."

Section 46(2) authorizes the Data Commissioner to "prohibit, suspend or subject the transfer to such conditions as may be determined." Though that authority is limited to instances where data subjects' rights and fundamental freedoms are at stake, that limitation – as stated – is ambiguous enough to allow for interpretations that could unintentionally undermine broader Kenyan and international interests.

Part VII – Exemptions

Section 47 *General Exemptions*

To support legally authorized information sharing between government agencies in Kenya and those in other countries, we recommend revising this section to explicitly exempt government-to-government transfers for government regulatory purposes, enforcement of civil or criminal laws, and for purposes of national security. Additionally, Section 47(2)(b), which provides an exemption when "disclosure is required by or under any a written law or by an order of the court," should include transfers required under laws or courts outside of Kenya.

Part X: Offences and Miscellaneous Provisions

Section 59. *General Penalty*

Section 59 provides for fines, imprisonment, and other penalties associated with violations of this draft bill. Criminal penalties – including imprisonment – are a departure from international norms and represent a potentially disproportionate penalty for a violation. Most privacy frameworks around the world depend on civil penalties to address violations, which generally impact the institution rather than the compliance staff. Holding individuals criminally accountable for violations – which may not have been intentional or egregious and are at the direction of their employer – may prevent highly qualified and competent individuals from accepting employment in support of the data protection practices of companies operating in Kenya. Limiting penalties to fines and ensuring penalties are tied to the intentionality of a data fiduciary's actions are more appropriate inclusions to the law. Effective enforcement of privacy laws is paramount, but the penalty should be proportionate to the offense.

Any questions or comments may be directed to: Michael Rose, Acting Director for Global Data Policy, Office of Digital Services Industries at the U.S. Department of Commerce's International Trade Administration, Michael.Rose@trade.gov, 202-815-0375.