KEY THREATS TO DIGITAL TRADE 2022

Middle East & Africa

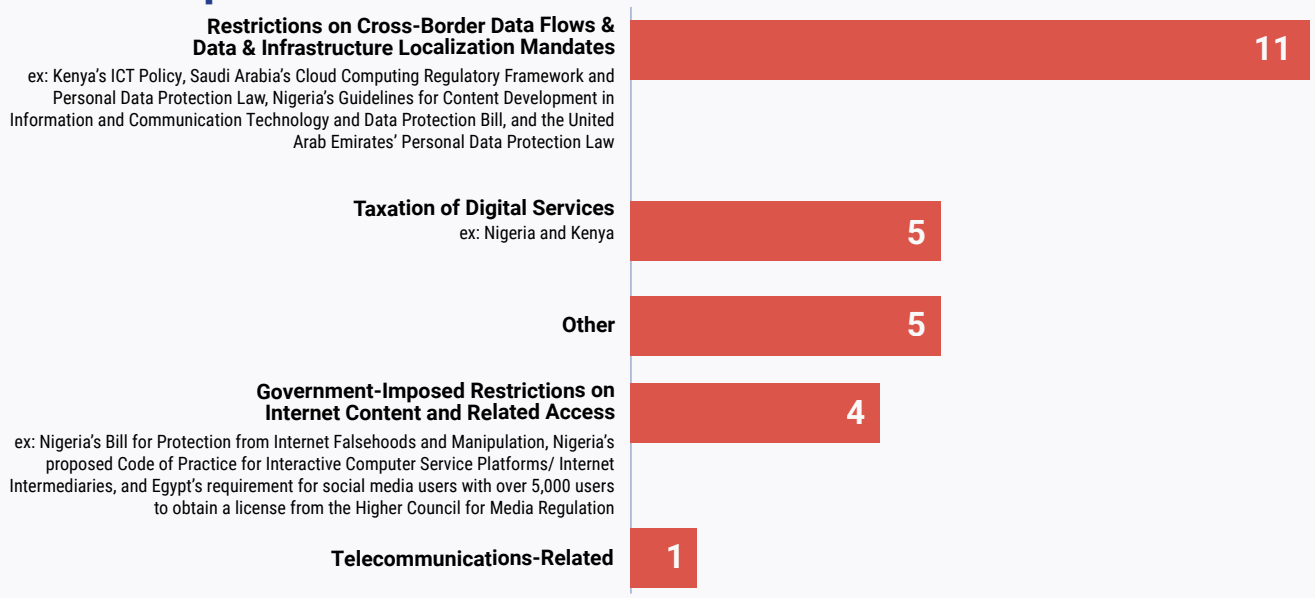
The United States has enjoyed strong diplomatic and economic relationships with the countries in the Middle East and Africa for decades. Services drive the modern benefits for U.S. exports in this mutually beneficial relationship, as are digital services. The U.S. generated **at least $13.6 billion in exports of digital services** to the region in 2021, bringing numerous positive externalities for business operations and consumers in the region and a **trade surplus of at least $1 billion** in the sector.

This region includes analysis of policies in Egypt, Kenya, Nigeria, Saudi Arabia, and the United Arab Emirates.

The United States has formalized its trading partnership and economic cooperation with countries in the region in several fora, including the African Growth and Opportunity Act, several bilateral treaties, and prior work around the Middle East Free Trade Area Initiative. As work is done to advance these initiatives, the United States should ensure partners do not restrict the ability of U.S. firms to enter or expand into their markets and engage in cross-border delivery of goods and services.

This engagement comes at a critical moment in the relationship. Countries in the Middle East and Africa have enacted policies that hinder the ability of U.S. digital services to operate. The following is excerpted from CCIA's annual comments submitted to the Office of the U.S. Trade Representative regarding its National Trade Estimate report—first, there are broad takeaways from the region followed by details of the trends identified in the region.

Key Threats to the U.S.-Middle East & Africa trading relationship in 2022



CCIA identified **26** digital trade barriers in the Middle East & Africa

18 policies have been enacted

8 are in development

Digital Trade Barrier Trends for the Americas in 2022.

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

- **Kenya**:
  - A new ICT Policy was released in August 2020, which includes a clause on "equity participation". The policy proposes an increase to 30 percent of the local ownership rules, currently set at 20 percent. The requirement would take effect by 2023. If these provisions were enacted, only firms with 30 percent "substantive Kenyan ownership" would be licensed to provide ICT services. Additionally, the ICT Policy requires that Kenyan data remains in Kenya, and that it is stored safely and in a manner that protects the privacy of citizens. This provision conflicts with the 2019 Data Protection Act, which enables cross-border data transfers subject to conditions set out by the Data Commissioner.
  - In 2021, the new Office of the Data Commissioner issued draft regulations proposing that data processed for the purpose of "actualising a public good" shall be processed in a server and data center based in Kenya. This would include, but not limited to, data related to civic registration and national identification systems; primary and secondary education; elections; health; electronic payments and public revenue administration.

- **Saudi Arabia:**
  - The Communications and Information Technology Council of Saudi Arabia (CITC) issued the Cloud Computing Regulatory Framework in 2018, with revisions made in 2019. The rules contain a provision on data localization that may restrict access to the Saudi market for foreign Internet services. The regulation will also increase ISP liability, create burdensome new data protection and classification obligations, and require compliance with cybersecurity and law enforcement access provisions that depart from global norms and security standards. CITC would be granted broad powers to require cloud and ICT service providers to install and maintain governmental filtering software on their networks.
  - The Personal Data Protection Law was passed in September 2021 and went into effect on March 23, 2022, with punishments for certain violations rising to 5 million riyals (approximately $1.33 million) and others leading to up to two years in prison. The law requires storing data in Saudi Arabia and requires any entity that seeks to store or process abroad to first conduct "an impact assessment and [obtain] the written approval of the Regulatory Authority after the Regulatory Authority has liaised with the Competent Authority on a base-by-case basis." Entities that seek to process personal data are required to register and pay an annual fee associated, and non-Saudi companies that process the personal data of Saudi residents are mandated to have a local representative. Data transfers outside of the country are only permitted in limited circumstances and with several restrictions on top of those lifted from GDPR and similar laws implementing adequacy assessments and a list of approved export markets. Firms may only process personal data without a user's express consent in limited instances, and individuals have the ability to rescind that consent—this lack of clarity over exceptions to data transfer restrictions represents confusion for businesses seeking to operate in Saudi Arabia.

- **Nigeria**:
  - Nigeria's 2013 Guidelines for Content Development in Information and Communication Technology establish local hosting requirements for government (sovereign), consumer and subscriber data, unless express approval has been obtained from the technology regulator (NITDA) for a cross-border transfer. This is in addition to 2011 Guidelines from the telecoms regulator requiring local hosting of subscriber data and from the Central Bank Guidelines requiring domestic routing of card transactions; the Central Bank Guidelines do not envisage the possibility of cross-border transfers.

- More recently, a Data Protection Bill, which looks to create a Data Protection Commission, seeks to regulate the collection, storage and use of personal data of data subjects in Nigeria. It requires that personal data be processed lawfully based on a legal basis. The Bill applies to entities in the private and public sector as well as data controllers and processors operating within and outside the country. It extends its applicability to personal and biometric data of data subjects; personal banking and accounting records; academic transcripts; medical and health records; telephone calls; messages, among other things. The application of the Bill exempts from its scope the processing of personal data by a data subject while carrying out purely personal or household activities.

- **United Arab Emirates**:
  - A new Personal Data Protection Law went into effect in January 2022 and will be enforced beginning November 2022. The is extraterritorial in scope and envelopes data controllers and data processors outside the UAE that happen to process UAE individuals' data. Personal data transfers abroad are permitted if the Data Office has approved that country for having an adequate level of protection. Transfers to countries not on this list are possible through user consent and contracts, among other options.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

- **Nigeria**:
  - A Bill for Protection from Internet Falsehoods and Manipulation was introduced in the Senate in December 2019. Beyond hate speech, the proposed law broadly criminalizes statements that may prejudice the country's security, public health, public safety, or friendly relations with other countries; or that may diminish confidence in the government. Online content service providers would also be subject to orders to disable access to the offending content or to issue 'correction notices' to all end users that may have had access to the content.
  - Nigeria's National Information Technology Development Agency posted draft regulations, dubbed the "Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries" in June 2022 which contain a wide spread of concerning government intrusiveness into online platforms' content moderation decisions, onerous takedown regimes, and localization requirements reserved only for "large" suppliers. The regulations would require platforms to take down content, once notified by a user or a government agency, unlawful content within 24 hours.
  - The regulations would also require platforms to reveal the identity of "the creator of information" on its service when demanded by a court order if it is for the "purpose of preventing, detecting, investigating, or prosecuting an offence concerning the sovereignty and integrity of Nigeria, public order, security, diplomatic relationships, felony, incitement of an offence relating to any of the above or in relation to rape, child abuse, or sexually explicit material."
  - The regulations would also impose monitoring requirements on platforms—under the term "due diligence" to ensure no unlawful content is uploaded to their services and a subsequent requirement to not only take down content when alerted by authorized government agencies but to also "ensure it stays down." This would be an unreasonably burdensome requirement to impose on online platforms while also infringing on individual users' privacy.

- **Egypt**:
  - In 2018, Egypt passed a new law that requires all social media users with more than 5,000 followers to procure a license from the Higher Council for Media Regulation. Reports continue to show the government's increased use of censorship, website blocking, and mandated content filtering.
  - In May 2020, Egypt's top media regulator issued Decree no. 26 of 2020 that enforces a strict licensing regime on Media and Press outlets. This includes online platforms. Under the regulation, there is a 24-hour timeline for removing harmful content. Further, international companies are obligated to open a representative office within the country, while naming a liable legal and content removal point of contact. There are no safe harbor protections for foreign companies, and the regulation stipulates an average of $200k in licensing fees (which could conflict with the existing Media law of 2018).

Taxation of Digital Services

- **Nigeria**:
  - The 2020 Finance Act introduces income tax obligations for non-resident companies providing digital goods and services in Nigeria. This policy was eventually signed into law as the Finance Act of 2021 on December 31, 2021. While the law applies to all non-resident companies earning above a certain threshold, extensive media coverage and analysis by experts has repeatedly mentioned the targeting of US multinationals. The law specifically references non-resident companies with a 'significant economic presence' in the country which is defined by a number of factors including: a minimum amount of revenue generated from users in Nigeria, transmitting data about Nigerian users, or the availability of local websites or local payment options. Exceptions have been built into the law for companies that are covered by a multilateral agreement to which the Nigerian government is a party.
  - Another form of taxation is developing in Nigeria, whereby the government requires all advertising of any kind to be approved by the Advertising Regulatory Council of Nigeria at risk of monetary punishment.

- **Kenya**:
  - Kenya implemented the following tax laws in 2020: (1) a 20 percent withholding tax on "marketing, sales promotion and advertising services" provided by non-resident persons; (2) a 1.5 percent digital service tax on income from services derived from or accruing in Kenya through a digital marketplace, and (3) a revision to the VAT liability of exported services from zero-rated to exempt, so that the services provided by the local entity to overseas entities would no longer be classified as services for export and the local entity would no longer claim VAT refunds on its costs for those services. Kenya has still not endorsed the OECD Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy.