February 26, 2018

Brief in Support of Written Testimony of ACT | The App Association to the United States International Trade Commission

Investigation No. 332-562
Hearing: Global Digital Trade 2: The Business-to-Business Market. Key Foreign Trade Restrictions, and U.S. Competitiveness;

Investigation No. 332-563
Global Digital Trade 3: The Business-to-Consumer Market, Key Foreign Trade Restrictions

I. Statement of Interest

ACT | The App Association appreciates this opportunity to testify before the U.S. International Trade Commission (USITC). The App Association is pleased to contribute its views as the USITC examines matters relevant to its investigation of foreign digital trade restrictions in both business-to-business and business-to-consumer contexts. The findings of the USITC will be essential to the U.S. Trade Representative moving forward.

The App Association represents more than 5,000 app makers and connected device companies across the country, and throughout the mobile economy. Our members leverage the connectivity of smart devices to create innovative solutions that make our lives better. The App Association leads globally in representing the small business software development community that seek to grow and create jobs into new markets abroad. Additionally, the App Association is a member of the Department of Commerce's Industry Trade Advisory Committee on Information and Communications Technologies, Services, and Electronic Commerce[1] where we frequently engage with the U.S. and other governments on digital trade matters. For example, the App Association recently provided detailed oral and written testimony to the U.S. International Trade Commission on digital trade barriers from the perspective of small business software developers and tech companies.[2]

[1] *See* http://www.trade.gov/itac/committees/itac08.asp.

[2] ACT | The App Association Comments to USITC, Investigation No. 332-561 (2017), *found here:* https://www.usitc.gov/press_room/documents/testimony/332_561_005.pdf.

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

As the world has quickly embraced mobile technology, the hyper-competitive app ecosystem—a global economy the App Association has recently valued at over $143 billion[3]—continues to produce more innovative and more efficient solutions that leverage mobile technologies to drive the global digital economy across modalities and segments, greatly augmenting consumer and enterprise interactions and experiences. This app ecosystem is led by U.S. companies, the vast majority of which are startups or small businesses.

The App Association's members engage in both the business-to-business and business-to-consumer markets across sectors and segments of the economy. The vast majority of the barriers our members face in entering foreign markets apply to both contexts, and for this reason we do not differentiate the barriers we describe generally (or give examples of in the pages following) in this brief.

While the global digital economy holds great promise for small app development companies that must continue growing to compete, our members face a diverse array of challenges entering new markets. These barriers may be laws, regulations, policies, or practices that either exclude U.S. goods and services from foreign markets, artificially stimulate exports of particular domestic goods and services to the detriment of U.S. companies, or fail to provide adequate and effective protection of intellectual property rights for U.S. companies. While these challenges take many forms, they have the same net effect: impeding U.S. exports and investment.

We urge the USITC to consider the implications of foreign barriers affecting U.S. exports of goods and services, U.S. foreign direct investment, and protection of intellectual property rights. The barriers we discuss below are typically most visible in key markets, such as China and the European Union. Ameliorating these concerns will promote the exponential growth of the app ecosystem spurred by small-business app companies in both domestic and foreign markets. The USITC's studies on both barriers in both the business-to-business and business-to-consumer contexts will be essential in efforts by the U.S. government to help U.S. small business innovators grow and create jobs.

[3] ACT | The App Association, *The State of the App Economy*, Report (2017), *found here*: https://actonline.org/wp-content/uploads/App_Economy_Report_2017_Digital.pdf.

II. General Principles

The App Association is committed to working with the USITC and other stakeholders to reduce or eliminate digital trade barriers. With respect to digital trade, the small business innovators that the App Association represents strongly urges the USITC to include the following priorities in its studies:

- **Facilitating Cross-Border Data Flows:** The seamless flow of data between economies and across political borders is essential to the functioning of the global economy. In order to grow their businesses and support more American jobs, innovative small app development companies, in particular, must be able to rely on unfettered data flows as they seek access to new markets.
- **Data Localization Policies:** Companies looking to grow in new markets too often face regulations that force foreign providers to build and/or use local infrastructure in-country. These data localization requirements cause serious declines in imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification. Our member companies do not have the resources to build, maintain, or use unique infrastructure in every country in which they may do business, and such requirements often effectively exclude them from commerce. With respect to data localization policies, the App Association is particularly concerned with requirements, some in place and others proposed, in other key markets, including Russia, China, and India.
- **Customs Duties on Digital Content:** American app developers and technology companies need to take advantage of the internet's global nature to reach the billions of new customers outside of the U.S. However, the "tolling" of data crossing political borders in order to collect customs duties directly contributes to the balkanization and reduced efficiency of the internet and effectively blocks these innovative products and services from market entry. We note that, since 1998, the World Trade Organization (WTO) has agreed to a moratorium on imposing customs duties on electronic transmissions.[4]
- **Requirements to Provide Source Code for Market Entry:** Some governments have put into place policies requiring companies to transfer or give access to proprietary source code before being able to legally enter that country's marketplace. For app developers and tech companies, intellectual property is the lifeblood of their innovation, and transfer of source code to a government presents an untenable risk of theft and piracy. These requirements are serious disincentives to digital trade and a non-starter for our members. In practice, such requirements lock small business software and tech innovators out of a market.

[4] https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm.

- **Prevent Public-Utility Style Regulations on Mobile Operating Systems:** Key markets have begun to implement policies that intend to treat mobile operating systems (OS) (e.g., iOS and Google Play) as public utilities.[5] These policies, in effect, place foreign governments in the middle of private negotiations between mobile platforms and app developers. Since its inception, the app economy has successfully operated under an agency-sale relationship that has yielded lower overhead costs, greater consumer access, simplified market entry, and strengthen intellectual property protections for app developers with little-to-no government influence. Foreign governments regulating OS as a public utility stand to frustrate this harmonious relationship enjoyed by small-business app developers and mobile platforms, which ultimately serves as a significant barrier of entry for our members in those countries.
- **The Ability to Use Strong Encryption Techniques to Protect End User Security and Privacy:** App economy innovators across the U.S. depend on technical data protection methods such as the use of strong encryption techniques to keep users safe from harms such as identity theft. However, some countries continue to demand that "back doors" be built into encryption for the purposes of government access. These policies would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. The viability of a small app development company's product from a security and privacy standpoint depends on the trust of its end users.
- **Protection of Intellectual Property:** The infringement and theft of intellectual property and trade secrets presents a major threat to the success of the App Association's members and, in turn, the billions of consumers who rely on these app-based digital products and services. These intellectual property violations can lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone a potential "end-of-life" occurrence for a small app development company. Strong, but fair, protection of intellectual property for copyrights, patents, trademarks, and trade secrets is essential.

We appreciate the USITC's investigation of business-to-business and business-to-consumer digital trade barriers. In further support of our views above, we offer a non-exclusive list of examples of trade barriers our members face across key markets that fall under the categories of trade barriers noted above.

We stand at the ready to assist USITC in its stated goals for this investigation.

[5] *E.g.*, ARCEP, *Devices, The Weak Link in Achieving an Open Internet*, Report (2018), *found here:* https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf.

CHINA

Proposed Internet Domain Name Management Rules

With more than 50 percent of its population online, China represents enormous potential for small business innovators to grow and and create new jobs while relying on the internet to reach new markets. The App Association's members face growing challenges to enter the Chinese market, including the internet regulatory regime in China. Attempts to filter or impede cross-border data flows continue to harm internet-related businesses and the consumers who use them.

We note that China's Ministry of Industry and Information Technology (MIIT) March 25, 2016-issued draft regulation titled "Internet Domain Name Management Rules (Opinion-seeking Revision Draft)"[6] which includes an article addressing China's power to not provide internet service to foreign internet sites, specifically states:

> Article 37: Domain names that connect to the network from within the borders shall have services provided by domestic domain name registration service bodies, and domestic domain name registration management bodies shall carry out operational management. For domain names that connect to the network from within the borders, but which are not managed by domestic domain name registration service bodies, internet access service providers may not provide network access services.

This article would allow any internet service provider in the country to block network access to a foreign website or internet-based business simply because their domain name is registered in a different country. The application of this regulation poses a significant threat that small business innovators from the App Association's membership may be selectively excluded from the Chinese marketplace to buoy domestic interests.

Cyberspace Administration of China (CAC) Mobile App Regulation

In June of 2016, the CAC released, without seeking public input, a regulation addressing mobile app providers and mobile app stores, titled "Administrative Provisions on Information Services of Mobile Internet Application Programs."[7] This regulation contains numerous provisions intended to protect national security through requirements on app providers such as requiring the monitoring of online content and the reporting of violations to government authorities, as well as ensuring that new app users register with their real identities; and the monitoring of and taking action against users that publish "banned content" as well as the reporting of the same to Chinese government authorities. This regulation went into effect on August 1, 2016.

---

[6] Rogier Creemers, *Internet Domain Name Management Rules (Opinion-seeking Revision Draft*, China Copyright and Media (last updated Mar. 29, 2016), *Available at* https://chinacopyrightandmedia.wordpress.com/2016/03/25/internet-domain-name-management-rules-opinion-seeking-revision-draft/.

[7] Cyberspace Administration of China, *Provisions on the Management of Mobile Internet Applications' Information Services*, (June 28, 2016). *Available at* http://www.cac.gov.cn/2016-06/28/c_1119123114.htm.

Cybersecurity Law

China has either put into effect or has proposed numerous restrictions on the flow of data across its borders. These proposed or final regulations limit or prohibit the transfer of data from within China in such areas as banking and financial credit, cybersecurity, counter-terrorism, commercial information systems, healthcare, and insurance. Each represents a significant barrier to market entry and is, effectively, a non-starter for small business innovators who would otherwise look to the Chinese marketplace to expand their businesses and create jobs.

In November 2016, China's Standing Committee of the National People's Congress passed final legislation imposing new cybersecurity data governance requirements on companies doing business in China. The law became effective on June 1, 2017. The law applies to both "network operators," defined as anyone owning or operating a computer system network, and "suppliers of network products and services."[8] The new law addresses a comprehensive array of privacy and security regulations. The Chinese government has stated that this law is intended to protect national security by better safeguarding Chinese citizens' data and giving law enforcement more access to technological systems when needed.

The most concerning aspect of the law is the vagueness of its text, leaving the scope of the law precariously undefined. What is definitive in the law's language is that it applies to all foreign technology companies conducting business in China. The law requires foreign technology and data companies to build or maintain servers inside of China, so that the data of all Chinese citizens will be stored exclusively within China. This demand for data localization effectively means that technology companies, including many of the App Association's members, may be simply priced out of doing business in the Chinese market.

This law also mandates that companies provide "technical support" to Chinese law enforcement during an investigation, but it does not clearly define what that entails. In some cases, technical support to law enforcement could consist of a "backdoor" to the technical protection mechanisms on which software companies heavily rely to maintain customer trust, like encryption. If companies are required to create such a "backdoor" in the process of an investigation, they face the possibility of an eroded global customer base.

Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data

On April 11, 2017, the CAC released a draft titled "Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data" for public comment (due May 11).[9] While the App Association continues to evaluate this proposal and will be submitting views directly to the CAC, our preliminary assessment of the proposal has raised significant concern regarding the subjectivity of this proposal as well as its mandating of all "network operators" to

[8] http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

[9] www.cac.gov.cn/2017-04/11/c_1120785691.htm.

self-assess the security of their cross-border data transfers and being subject to similar assessments by the Chinese government.

Mandates for Source Code Disclosure/Escrow

While, during its accession to the WTO, China committed to not make foreign direct investment and market access opportunities dependent upon technology transfer requirements, such practices unfortunately continue to this day. We are aware of instances of joint venture requirements, foreign equity limitations, ambiguous regulations and regulatory approval processes, and other creative means (such as source code "escrowing") that force foreign companies to transfer IP to access the Chinese market. These practices are a present and ongoing concern for our members, and likely constitute violations of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the Agreement on Trade-Related Investment Measures (TRIMs).

Virtual Private Network Restrictions

A virtual private network (VPN) creates a safe and encrypted connection to the internet. Applications running on a VPN benefit from the functionality, security, and management of the private network.[10] China regulates and restricts the use of VPNs, leaving consumers in China out of the digital marketplace, while creating massive barriers to entry within the tech industry. China's "extensive blocking of legitimate websites" also threatens to impose significant costs on providers and users of services and products.[11] The App Association has keen interest in this policy because it creates a serious disincentive for our members when considering whether to enter the Chinese market or pursue different business ventures.

EUROPEAN UNION

General Data Protection Regulation

As we described in our guideline,[12] the European Union's General Data Protection Regulation (GDPR) poses a significant barrier of entry for many of our members. For example, Article 3 of the GDPR is clear that the regulation is extraterritorial in nature.[13] This includes its hefty penalties, which maintains a maximum penalty of the greater of 4 percent of a company's total global revenue or €20 million.[14] For a small business app company, this penalty could spell death for all those that wish to do business in the EU. Additionally, the GDPR requires a physical representation in the EU for those companies not based in an EU member state if that company

[10] Mason, Andrew G. (2002). *Cisco Secure Virtual Private Network.* Cisco Press. P. 7.

[11] Pham, Sherisse, *China says VPN crackdown aimed at 'cleaning' the internet,* (July 25, 2017), *available at* http://money.cnn.com/2017/07/25/technology/china-vpn-censorship/index.html

[12] http://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf.

[13] Art. 3(1) GDPR.

[14] Art. 83(6) GDPR.

processes EU data subjects' personal information more than occasionally.[15] However, the EU has yet to define what the term "occasionally" means in this context.

Our members are also concerned with the enforcement of Article 48, while adhering to U.S.-based warrants. The issue arises when U.S. law enforcement agencies request data from companies that store data in the EU and request such data under the Email Privacy Communications Act without going through proper procedures and channels pursuant to international law. At that point, the U.S. government places any company in a Catch-22, where you either adhere to an ECPA warrant or potentially violate the GDPR by not going through an multilateral assistance treaty (MLAT) process—a process the U.S. has with every EU member. Such a choice would dissuade any of our members in engaging with the EU moving forward.

The matter is further complicated with European Commission (EC) publishing conflicting viewpoints on Article 48 and its relationship with Article 49. For example, the EC filed an *amicus curiae* in the *U.S. v. Microsoft* case where it claimed that Article 49 of the GDPR could circumvent the requirements codified in Article 48.[16] It almost suggests that Article 49's public interest exception swallows the rule under Article 48 that requires the U.S. government to go through an MLAT process, because solving crime is in the public interest.[17] Compare this with the Working Party 29 and EU Data Protection Authorities that have stated outright in other contexts that foreign interests alone do meet the public interest test.[18] These conflicting interpretations cause many of our members pause when deciding to engage in EU markets.

ePrivacy Regulation

Concurrent to the GDPR, the EU's E-Privacy Regulation goes into effect on May 25, 2018. In effect, the E-Privacy Regulation is an extension of the so-called "cookie" law that intends to augment those restrictions to apply to the entire internet ecosystem. The concept is that the ePrivacy Regulation serves as a *principe lex specialis* meant to compliment and, at times, override the GDPR—a *lex generalis* regime—in particular circumstances. However, the looming enactment of the GDPR at the same time as the ePrivacy Regulation complicates our members' ability to comply with either set of rules, because now our members now have two sets of regulations with varying standards attempting to monitor the same behavior. The issue mainly arises in the ambiguity as to what law controls at what time. For a small business app company it would inevitably cost an exorbitant amount of money in legal fees and time to ensure they are compliant with both the GDPR and the EU's ePrivacy Regulation. Thus, this regulation will serve an important consideration for our members when deciding to enter into EU markets.

Threats to Encryption

[15] Art. 27 GDPR.

[16] European Commission Amicus Br. 15-16.

[17] *See id.*

[18] *E.g.*, https://www.dataprotection.ie/docs/Transfers-Abroad/y/37.htm; *see* also, Working Document 114 of the WP29 (2005).

European Justice Commissioner Věra Jourová announced on March 28th that the European Commission will release related rules on June 20th, 2017, that will grant law enforcement easier access to end-to-end encrypted data on electronic communications services like WhatsApp.[19] This follows public calls from officials in the United Kingdom, Germany, and France for law enforcement to have the same rights to access encrypted online services as they do to phone call information from telecommunication companies during criminal investigations.

The approach proposed by Commissioner Jourová is seriously flawed from both a policy and a technical perspective. Any transaction involving data depends on technical data protection methods, such as the use of strong encryption techniques, to maintain user trust. Mandating the development of "backdoors" into encryption frameworks for the purposes of government access would not only degrade the safety and security of data, but also jeopardize the trust of end users by creating known vulnerabilities that unauthorized parties can exploit. Undermining the technical proficiency of encryption moves us away from, rather than towards, the legitimate policy goals that the App Association supports, including law enforcement's proper and timely access to data.

INDIA

Data Localization

India has in place, and is considering, policies that restrict the flow of data across its borders and create significant issues for small business innovators seeking to expand into the Indian market, including:

- India's National Data Sharing and Accessibility Policy requires that all data collected using public funds to be stored within the borders of India.[20]
- The 2015 National Telecom M2M ("machine to machine") Roadmap,[21] which has not been implemented, states that all M2M gateways and application servers serving customers in India need to be located within India. The draft policy also proposes that foreign SIM cards should not be permitted in devices to be used in India.

Regulations on Encryption

Currently, Indian internet providers must attain government approval from the Telecom Regulation Authority of India (TRAI) to employ encryption stronger than 40-bit encryption. Laws like this provide fewer touchpoints for our members' apps to reach consumers. Although we are not primarily affected by the regulation, it affects American business and must be

[19] *See* Eurativ, "EU to propose new rules targeting encrypted apps in June," (Mar. 29, 2017), *available at* http://bit.ly/2phYX3C.

[20] Government of India Ministry of Science & Technology, *India's National Data Sharing and Accessibility Policy*, (2012). *Available at* http://ogpl.gov.in/NDSAP/NDSAP-30Jan2012.pdf.

[21] Government of India Ministry of Communications & Information Technology Department of Telecommunications, *National Telecom M2M Roadmap*. *Available at* http://www.gsma.com/connectedliving/wp-content/uploads/2015/05/150513-DoT-National-Telecom-M2M-Roadmap.pdf.

considered as a trade barrier. Further, as recently as late 2015, the Indian government proposed a National Encryption Policy that presented numerous proposals of significant concern to the App Association. This is an ongoing issue of serious concern to small business innovators

Privacy Regulation

The Indian government has sought to regulated digital privacy using at least a couple of forums in a concerning manner. The first is through its primary telecommunications regulator the Telecom Regulatory Authority (TRAI). In 2017, the TRAI published a consultation seeking public comment on whether it should institute sweeping privacy regulations over India's telecommunications carriers akin the GDPR or the U.S. Federal Communications Commission's (FCC's) consumer proprietary network information rules—now repealed by Congress via Congressional Review Act.[22] In response to its call for comment, the App Association cautioned the TRAI of the potential harms to small business app developers has on enacting such a measure. Further, we strongly urged for the TRAI to exempt small businesses from adherence to any such privacy regime to ensure that these key innovators are not driven out of business by the cost of compliance.

More recently, the Indian government's Ministry of Electronics and Information Technology (MeitY) placed a call for comment for its consultation on developing a legal framework for e-privacy more generally.[23]

INDONESIA

Data Localization Requirements on Electronic System Providers of Public Services

Indonesia's Ministry of Communications and Information Technology (MCIT) has enacted regulations that require electronic system providers for public services to locate a data center and disaster recovery center within Indonesia.[24] These data localization laws cover a broad and expanding range of sectors and technologies. In 2012, Indonesia enacted regulation no. 82,[25]– regarding the provision of Electronic Systems and Transactions, which requires "electronic systems operators for public service" to store data locally. Indonesia has also implemented regulations regarding e-payments and the local storage of financial data. While larger companies

---

22 http://www.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf.

23 http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf.

24 *See* Mary R. Silaban, *Unleashing Indonesia's Digital Innovation*, American Chamber of Commerce in Indonesia (June 10, 2014), *available at* http://www.amcham.or.id/fe/4614-unleashing-indonesia-s-digital-innovation. *See also*, U.S. Dep't of State Bureau of Economic and Business Affairs, *2014 Investment Climate Statement – Indonesia*, (June, 2014), a*vailable at* http://www.state.gov/documents/organization/226821.pdf.

25 Vasey, Kay, *Indonesia moves towards comprehensive data law – how will it impact your business?*, CMS UK Datonomy Blog (July 4, 2017) *available at http://datonomy.eu/2017/04/07/indonesia-moves-towards-comprehensive-data-law-how-will-it-impact-your-business/*

possess the ability to absorb these costs to provide their products and services to the Indonesian consumers and businesses, these requirements pose a massive disincentive for the App Association's small tech innovators. The especially broad implications are evident in the language that it covers "personal data" and applies to "any institution that provides information technology-based services".[26]

Proposed Regulations on "Over the Top" Service Providers

The App Association has significant concern with the Ministry of Communication and Informatics' (Kominfo) *Draft Regulation of the Minister of Communications and Information of the Republic of Indonesia, Number ___ of 2016, concerning Provision of Application Services and/or Content over the Internet (OTT)*.[27] We believe that the proposal, when implemented, will create an overly burdensome regulatory environment in a number of ways that will hamper economic growth for Indonesia, including Indonesia's burgeoning mobile app developer business community. This publicly-proposed Kominfo regulation, with which we have significant concern, includes:

- Requiring a physical presence in Indonesia by OTT service providers when small businesses simply can neither afford to open local offices in every market in which they offer their services, nor can they afford to dedicate resources to establishing partnerships with local conglomerates. This requirement would create a cost burden to market entry that is untenable for small businesses, particularly in the case of attaining licensing from the Investment Coordination Board.
- Mandatory partnerships between OTT service providers and telecommunication providers, when such a policy would be extremely expensive for all OTT service providers (as defined by Kominfo), and particularly onerous for small app makers.
- Requiring the localization of data storage or processing, specifically (1) the use of national payment gateways that are legally incorporated in Indonesia, specifically for paid OTT [services]; (2) the use of an Indonesian internet protocol number and place part of the server in data centers in Indonesia; and (3) the local storage of data for a minimum of three (3) months, or longer should law enforcement request it.

On May 26, 2016, the App Association filed detailed comments with Kominfo describing the difficulties posed by many of the specific provisions in the draft OTT regulation, which we urge the Trade Policy Staff Committee to review.[28] Further, we respectfully requested that Kominfo

[26] *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?,* Information Technology & Innovation Foundation (May 1, 2017), *available at* https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

[27] Republic of Indonesia's Ministry of Communication and Information Technology, *Draft Number 3 of 2016 concerning Provision of Over-The-Top Application and/or Content Services via the Internet,* (Mar. 31, 2016), *available at* http://www.lexology.com/library/detail.aspx?g=4aa11c3e-cf65-4998-921a-2ac8408b375b.

[28] ACT | The App Association, *RE: Kominfo's Draft Regulation, Number ___ of 2016, Provision of Application Services and/or Content over the Internet (OTT),* (May 26, 2016), *available at* http://actonline.org/wp-content/uploads/act_comments_to_kominfo_re_draft_ott_regulation_052616-1.pdf.

refrain from implementing this regulation and engage in further consultation with affected stakeholders to allow for meaningful and win-win solutions to concerns that Kominfo may have in seeking to regulate OTT services.

We understand that the goal for the Indonesian government is to have OTT regulations finalized and in effect by the end of 2017. Although a new informal draft appears to make some improvements (e.g., no longer requiring a partnership with local telecom, stepping back from data localization mandates), no formal consultation has been initiated by Kominfo, and we continue to face great uncertainty as to the path forward for small business app developers in Indonesia. While this regulation remains in draft form, it remains of high concern to our members.

NIGERIA

The Nigerian government issued its "Guidelines for Nigerian Content Development in Information and Communications Technology,"[29] which raise a myriad of concerns for our members. The Nigerian government imposes extreme localization requirements on multinational companies. For instance, section 10.3 of the Nigerian government's guidelines mandates multinational companies to not only store their data in Nigeria but also requires such companies to incorporate 50 percent of local products when manufacturing ICT devices in the region. Moreover, it requires companies to hire local engineers when manufacturing such products.

These requirements are antithetical to advancing a vibrant and sustainable ICT marketplace. Many view Nigeria as a leader in the ICT space for the African Union (AU), and, if these guidelines become accepted rules of the road for the AU at large (or beyond), then it does not bode well for U.S. companies seeking to enter the African market. This poses a stark barrier for U.S. trade in the ICT economic ecosystem.

RUSSIA

Data Localization

Federal Law No. 242-FZ, signed by President Vladimir Putin in July of 2014, requires companies that store and process the personal data of Russian citizens to maintain servers on Russian soil and to notify the federal media regulator, Roskomnadzor, of all server locations.[30] It empowers Roskomnadzor to block websites and to maintain a registry of data violators. Additionally, in August 2015 a non-binding clarification suggesting that localization might apply to websites that include built-in Russian-language options, transact in Russian rubles, or use a Russian top-level domain such as .r.[31] The Roskomnadzor has used this law to block internet access within Russia to the website LinkedIn, for not following the data localization requirements sufficiently.[32]

In July of 2016, a package of amendments was released imposing extensive data storage requirements on telecommunications providers and companies classified as internet telecommunications services.[33] Per these changes, telecom operators must store metadata for three (3) years and internet telecoms for one (1) year, while both must retain the content for up to six (6) months. Companies will have until July 1, 2018, to begin implementing these

[29] NITDA, *Guidelines for Nigerian Content Development in Information and Communications Technology* (2017).

[30] Russian Federation, *Federal Law No. 242-FZ*, (July 21, 2014). *Available at* https://pd.rkn.gov.ru/authority/p146/p191/.

[31] Russian Federation's Ministry of Communications and Mass Media, *Clarifying Federal Law No. 242-FZ*, (Aug. 3, 2015). *Available at* http://www.bna.com/russia-clarifies-looming-n17179934521/.

[32] https://www.insideprivacy.com/cross-border-transfers/linkedin-blocked-in-russia-following-breach-of-data-localization-laws/

[33] Russian Federation, "*Yarovaya Package" Federal Law No 374-FZ*, (July 6, 2016). *Available at* http://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

requirements. Moreover, if the stored messages and files are encrypted, companies will be required to provide Russian state security services with decryption keys upon request. In August 2016, Russia's Federal Security Service (FSB) announced that it has the capability to obtain information necessary for decoding the electronic messaging received, sent, delivered, and (or) processed by users of the internet.[34]

Further, on February 7, 2017, President Putin signed amendments to the Russian Code on Administrative Offences that increases fines for those violating Russian data protection laws. Effective on July 1, 2017, fines were raised substantially from RUB 10,000 to 75,000 or from approximately $170 to $1,260. [35] By raising the penalties for not abiding by this regulation, it is making it even harder to take a risk and creates additional barriers to digital trade and market entry.

Regulations on Encryption

Under Russia's current System of Operative-Investigative Measures (SORM), Russian ISPs must install a special device on their servers to allow the FSB to track all credit card transactions, e-mail messages, and web use. In 2014, SORM usage was extended to monitoring of social networks, chats, and forums, requiring their operators to install SORM probes in their networks. Further, advances of the SORM force online communications providers to provide the authorities with a means to decrypt users' messages, a technically infeasible result when end-to-end encryption methods are used. This law presents serious issues for small business innovators seeking to enter the Russian marketplace to compete.

Various Virtual Private Network Restrictions

On November 1, 2017, Russia will enact regulations that prohibit consumers' ability to use VPNs to access websites as an anonymous browser. The Russian government cites this regulation as an effort to keep people from accessing dangerous and illegal content. This regulation says that any internet providers that allow these to exist, or function without being blocked, will lose their market access. This is an obvious trade barrier and very real threat to the free market.

Additionally, there are new regulations regarding the anonymity of citizens while using chat apps such as Whatsapp or Facebook Messenger. Regulations going into effect on January 1, 2018, require these apps to provide the users' phone numbers to limit or prohibit access to those attempting to spread illegal content. Therefore, there is no ability to remain anonymous when using these applications. Although this is done under the veil of safety for citizens, it restricts the free flow of information and provides an extremely tough trade barrier to infiltrate.

[34] Federal Security Service of the Russian Federation, *Encryption Keys*, (Aug.1, 2016). *Available at* http://www.fsb.ru/fsb/science/single.htm!id=10437866@fsbResearchart.html.

[35] Hogan Lovells, *Chronicle of Data Protection,* "Russia Increases Fines for Violations of Data Protection Laws", (February 9, 2017), *available at* http://www.hldataprotection.com/2017/02/articles/international-eu-privacy/russia-increases-fines-for-violations-of-data-protection-laws/

TURKEY

Turkey's E-Payment Law requires the processing of e-payments occur within Turkey.[36] Even more recently, Turkey's Banking Regulation and Supervising IndUSITCy (BDDK) initiated a policy in mid-2016 that mandates that companies locate their ICT systems in the country.[37] These data localization requirements have chilled plans that the App Association's members have or would have to enter this important market should their app include e-payment capabilities.

VIET NAM

Originally proposed in June 2017, the Viet Nam's Ministry of Public Security has proposed a new cybersecurity law.[38] This law's intent is based in public interest yet is too broadly scoped; in addition, the law proposed to apply to onshore and offshore companies/individuals directly involved or related to the management, provision or use of cyberspace; imposes forced localization (specifically, administrators of critical systems must store personal data and critical data within Vietnam); imposes discriminatory licensing requirements; and conflicts with Viet Nam's pro-innovation and investment positions at APEC.

[36] U.S. Dep't of State Bureau of Economic and Business Affairs, *2016 Investment Climate Statement – Turkey* (July 5, 2016). *Available at* http://www.state.gov/e/eb/rls/othr/ics/2016/eur/254425.htm.

[37] Turkey's Banking Regulation and Supervising Industry (BDDK), *Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions numbered 6493*, Official Gazette numbered 28690, (published June 27, 2013). *Available at* https://www.bddk.org.tr/websitesi/english/Legislation/129166493kanun_ing.pdf.

[38] *See* http://www.bakermckenzie.com/en/insight/publications/2017/08/new-draft-cybersecurity-law-2017/.

The App Association submitted comments directly to MIIT, as well as through the TBT Committee, discussing our views on the above proposals[39] and how this proposed regulation's definitions and overly-prescriptive approach, if implemented, would risk restraining the highly-competitive and innovative mobile phone and app marketplace in China and will negatively affect the global digital economy.

Sincerely,

Brian Scarpelli
Senior Policy Counsel

Joel Thayer
Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005

[39] ACT | The App Association, *RE: Interim Administration Regulation for Mobile Smart Terminal Application Software Pre-installation and Distribution*, (June 6, 2016). *Available at* https://actonline.org/wp-content/uploads/MIIT-Pre-Installated-App-Regulation-.pdf.